

AD-A047 072

OHIO STATE UNIV COLUMBUS DEPT OF MATHEMATICS  
COMBINATORIAL SYSTEMS.(U)  
MAR 73 D K RAY-CHAUDHURI

F/G 9/4

UNCLASSIFIED

N00014-67-A-0232-0016  
NL

OF 2  
AD-A047 072



AD A047072

Log  
044-436

OSU RF Project 3430-A1  
Report No. 1

THE OHIO STATE UNIVERSITY



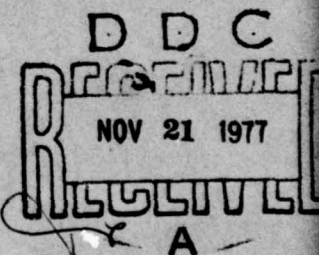
# RESEARCH FOUNDATION

1314 KINNEAR ROAD COLUMBUS, OHIO 43212

COMBINATORIAL SYSTEMS

Dr. D. K. Ray-Chaudhuri  
Department of Mathematics

7 March 1973



DEPARTMENT OF THE NAVY  
Office of Naval Research  
Arlington, Virginia

Contract No. N00014-67-A-0232-0016

AD No. \_\_\_\_\_  
DDC FILE COPY

16 APR 1973



RF Project. 3430-A1

Report No. 1

ANNUAL PROGRESS

# REPORT

By

THE OHIO STATE UNIVERSITY  
RESEARCH FOUNDATION

1314 KINNEAR RD.  
COLUMBUS, OHIO 43212

To DEPARTMENT OF THE NAVY  
Office of Naval Research  
Arlington, Virginia 22217

Contract No. 15 N00014-67-A-0232-0016

On 2 COMBINATORIAL SYSTEMS

9 Annual progress rept. no. 1,  
For the period 1 June 1972 - 31 Mar 1973

Submitted by 10 Dr. D. K. Ray-Chaudhuri  
Department of Mathematics

Date 11 7 Mar 1973

12 191p.

DDC  
RECEIVED  
NOV 21 1977  
RECEIVED

406019

ACCESSION FOR	
NTIS	White Section <input checked="" type="checkbox"/>
DDC	Buff Section <input type="checkbox"/>
UNANNOUNCED	<input type="checkbox"/>
JUSTIFICATION	
BY <u>RTI 1006</u>	
DISTRIBUTION AVAILABILITY CODE	
<u>Ver. by 1006</u>	
BIBL. AVAIL. NO. OR SPECIAL	
A	

## COMBINATORIAL SYSTEMS

Significant progress is made towards the completion of the ONR contract during the period June 1, 1972 through March 31, 1973. Professors D. K. Ray-Chaudhuri and T. A. Dowling, Dr. Xavier Hubaut, Dr. R. P. Gupta, Mr. Paul Catlin, Mr. Michael E. Segal and Mrs. Joan Smoot made research contributions in the fields of Information Retrieval, Combinatorial Geometries, Combinatorial Designs, Graph Theory, Coding Theory, and the Theory of Association Schemes.

Professor D. K. Ray-Chaudhuri worked on the problem of construction of "locally structured information retrieval systems". In most files, most of the documents (or items) possess only a small fraction of the attributes. The philosophy of local structuring is to take advantage of this fact. Local structuring partitions a large file into several small files such that to retrieve the items for a given query it will be necessary to search only a few of these small files. Construction of local structuring is based on  $(n,k,t,b)$  - combinatorial configurations. Several families of such configurations are constructed and their applications are being developed. A paper on these results is under preparation.

During the summer, 1972, a working seminar on Hypergraphs was held at The Ohio State University under the leadership of Professors Claude E. Berge and D. K. Ray-Chaudhuri. Professor Ray-Chaudhuri will be one of the editors of the Proceedings of the Hypergraph Conference to be published by Springer-Verlag.

Professor D. K. Ray-Chaudhuri was invited to present papers in the following International meetings

1. International Conference on Combinatorics and Its Application, New Delhi, December 22-24, 1972
2. Conference on Combinatorics, Oberwolfach, W. Germany, March 25-31, 1973.
3. International Conference on Combinatorics organized by the Bolyai Janos Mathematical Society in honor of the 60th birthday of Paul Erdős, Budapest, June 25-30, 1973
4. International Colloquium on Combinatorial Theory organized by the American Mathematical Society and the Accademia Nazionale dei Lincei, Rome, September 3-15, 1973
5. Combinatorics Colloquium at the University of Waterloo, Ontario, Canada, March 18-25, 1973.

Professor Ray-Chaudhuri will publish papers in the proceedings of the Budapest Conference and the Rome Conference.

Professor T. A. Dowling, jointly with Professor R. M. Wilson proved the following theorems for geometric lattices: Let  $L$  be a finite geometric lattice of rank  $r$  with  $n$  points. For  $k = 0, 1, \dots, r$ , let  $W_k(L)$  denote the number of elements of rank  $k$  in  $L$ . Then

$$W_k(L) \geq \binom{r-2}{k-1}(n-r) + \binom{r}{k}$$

Equality holds for some  $k$ ,  $2 \leq k \leq r-2$  if and only if  $L$  is a direct product of a modular plane and a Boolean algebra. Also for  $1 \leq k \leq r-2$ ,  $W_1 + W_2 + \dots + W_k \leq W_{r-k} + W_{r-k+1} + \dots + W_{r-1}$  with equality if and only if  $L$  is modular. The work of Professor Dowling was supported by the ONR contract. Two papers on this work are under preparation.

Dr. Xavier Hubaut, jointly with Dr. Wilson discovered two infinite families of symmetric 2-designs. The parameters of these designs are

$$i. \quad v = q(q^n - 1) + 1, \quad k = q^n, \quad \lambda = q^{n-1},$$

where  $q$  and  $q-1$  are prime powers;

and

$$ii. \quad v = 2q + 1, \quad k = q, \quad \lambda = \frac{1}{2}(q-1)$$

where  $q$  is a prime power.

These designs provide optimum experimental plans. Dr. Hubaut is working as a research associate for the ONR contract.

Mr. Michael E. Segal wrote an excellent Master's thesis, "Upper and Lower Bounds for Unrestricted Binary Error Correcting Codes". His exposition of coding theory will be very valuable to anyone working on the subject of coding theory. Mr. Segal's work was partially supported by the ONR contract.

Mr. Paul Catlin made important contributions to graph theory. Mr. Catlin was supported as a graduate research associate by the ONR contract. Mr. Catlin proved the following theorems.

Theorem: Let  $G(I, X)$  and  $H(J, Y)$  be bipartite graphs with  $|I| = |J|$  and  $|X| = |Y|$ . Let

$$d = \max_{v \in J \cup Y} \deg_{H(I, Y)}(v).$$



Suppose there exist real numbers  $s$  and  $t$  satisfying

$$(1 - s)|X| \leq \text{Min deg}_{G(I,X)}(i) \quad , \quad i \in I ,$$

$$(1 - t)|I| \leq \text{Min deg}_{G(I,X)}(x) \quad , \quad x \in X ,$$

$$d(s|X| + t|I|) \leq |X| .$$

Then  $H(J,Y)$  is isomorphic to a subgraph of  $G(I,X)$ .

Theorem: Let  $G$  and  $H$  be simple graphs on  $p$  vertices and let  $d$  denote the maximum degree of vertices of  $H$ . If

$$\text{deg}_G(v) \geq p \left( 1 - \frac{1}{2d(d+1)} \right) - 1$$

for every vertex  $v$  of  $G$ , then  $G$  has a subgraph isomorphic to  $H$ .

Mr. Catlin also obtained theorems about the number of 1-factors of  $n$ -connected graphs. Mr. Catlin's theorems are simple and elegant and surely will find applications.

Dr. R. P. Gupta is working as a research associate for the ONR contract. He proved the following beautiful theorem about Hypergraphs.

Theorem: Let  $H$  be a balanced hypergraph. Then  $\forall k \geq 0$ ,  $\exists$  a  $k$ -coloration

$$\sigma \in V(H), \quad \sigma: X = X_1 \cup X_2 \cup \dots \cup X_k$$

such that  $v(E, \sigma) = \text{Min}\{k_i | E\}$  for all edge  $E$  of the hypergraph. Here  $v(E, 0)$  denotes the number of integer  $i$  for which  $1 \leq i \leq k$  and  $|E \cap X_i| > 0$ .

A paper is being written by Dr. R. P. Gupta.

Joan E. Smoot wrote a Master's thesis on three-class association schemes. Association schemes arise in the theory of Combinatorial Design. Joan Smoot obtained an economical description of the parameters of the three class association schemes. Her work was partially supported by the ONR contract.

Contents:

#### Appendices

1. "Some Applications of Transversal Theory to Graph Theory;" Paul A. Catlin, Masters Thesis, The Ohio State University (1973).
2. "Upper and Lower Bounds for Unrestricted Binary Error Correcting Codes;" Michael Ellis Segal, Masters Thesis, The Ohio State University (1973).
3. "Three-Class Association Schemes on a Small Number of Vertices." Joan Ericson Smoot, Masters Thesis, The Ohio State University (1972).

APPENDIX I

SOME APPLICATIONS OF TRANSVERSAL THEORY  
TO GRAPH THEORY

A Thesis

Presented in Partial Fulfillment of the Requirements  
for the Degree of Master of Science

by

Paul A. Catlin, B.S.  
The Ohio State University  
1973

Approved by

---

Advisor, Department  
of Mathematics



### Acknowledgments

The author wishes to thank Dr. Neil Robertson for his helpful assistance in the preparation of this thesis.

This work was supported by the ONR contract #N00014-67-A-0232-0016(OSURF3430A1).

## Table of Contents

	<u>Page</u>
Acknowledgment	11
Introduction	1
Results from transversal theory	3
Subgraphs of bipartite graphs	6
Subgraphs of simple graphs	13
The number of 1-factors of a graph	19
The 2-factors of graphs	28
References	33
Figure 1	34

1. Introduction. Throughout this thesis, all graphs considered are finite and simple. Given a graph  $G$ , the degree of a vertex  $v$  in  $G$  is denoted  $\deg_G(v)$ . The notation  $G(I,X)$  denotes a bipartite graph with an ordered partition of the vertex set into sets  $I$  and  $X$ . Likewise,  $H(J,Y)$  is a bipartite graph with vertices partitioned into sets  $J$  and  $Y$ . The vertex set of a graph  $G$  is denoted  $V(G)$ , and its cardinality is denoted  $p$ . The cardinality of a set  $S$  is denoted  $|S|$ . We say that the graph  $H$  can be embedded into the graph  $G$  if there is an injection  $\varphi: V(H) \rightarrow V(G)$  such that if  $v$  and  $w$  are adjacent in  $H$  then  $\varphi(v)$  and  $\varphi(w)$  are adjacent in  $G$ . However, in the case of bipartite graphs, we say that a graph  $H(J,Y)$  can be embedded in  $G(I,X)$  if there are injections  $\pi: J \rightarrow I$  and  $\varphi: Y \rightarrow X$  such that if  $j \in J$  and  $y \in Y$  are adjacent in  $H(J,Y)$ , then  $\pi(j)$  and  $\varphi(y)$  are adjacent in  $G(I,X)$ .

In the next section we state results from transversal theory which will be used.

In section 3, we apply a theorem of Rado from transversal theory to give a sufficient condition for an arbitrary bijection  $\pi: J \rightarrow I$  to be extended to an embedding of  $H(J,Y)$  into  $G(I,X)$ . We show that our result is best possible.



In section 4, we apply the result of section 3 to show that for any graphs  $G$  and  $H$  there is a constant  $c_d < 1$ , depending only upon

$$d = \max_{v \in V(H)} \deg_H(v),$$

such that if  $\deg_G(v) \geq c_d p - 1$  for all  $v \in V(G)$ , then  $H$  can be embedded into  $G$ . For certain graphs  $H$  with  $d = 2$ , this constant is  $7/8$ . The constants are not best possible.

I. Anderson [1] has given an elegant proof of Tutte's Theorem [10] characterizing graphs with 1-factors (spanning regular subgraphs of degree 1) using the well-known theorem of P. Hall [6], stated below, from transversal theory. Using a stronger theorem of M. Hall [5], in section 5 we shall derive some lower bounds on the number of 1-factors in a graph.

Finally, in section 6, we apply the same theorems of transversal theory to problems concerning 2-factors (spanning regular subgraphs of degree 2). In particular, we use P. Hall's theorem to improve a theorem of Petersen [8] characterizing graphs which are the edge-disjoint unions of 2-factors.

2. Results from transversal theory. As a reference, one may use Mirsky's book [7] for the results of this section. The first two theorems are used in sections 5 and 6. Let  $Z_m = \{1, 2, \dots, m\}$ .

Theorem 1 (P. Hall [6]) Given a family  $\mathcal{A} = (A_i: i \in Z_m)$  of subsets of a set  $X$ , a necessary and sufficient condition that a system of distinct representatives (SDR's)  $\{x_1, x_2, \dots, x_m\}$  of the sets of  $\mathcal{A}$  exist, where  $x_i \in A_i$  for all  $i$ , is that for any subset  $I'$  of  $Z_m$ ,

$$\left| \bigcup_{i \in I'} A_i \right| \geq |I'|.$$

Theorem 2 (M. Hall [5]) Given the notation of Theorem 1, if  $|A_i| \geq n$  for all  $i \in Z_m$ , where  $m \geq n$ , and if there is an SDR of  $\mathcal{A}$ , then there are at least  $n!$  different SDR's.

Throughout the rest of this section and in sections 3 and 4, lower case letters  $i, j, x, y$  will be used to denote vertices of the bipartite graphs  $G(I, X)$  and  $H(J, Y)$ , with  $i \in I$ ,  $j \in J$ ,  $x \in X$ ,  $y \in Y$ . Let  $X_i$  denote the set of vertices of  $X$  adjacent to the vertex  $i \in I$ . Likewise, let  $I_x$ ,  $Y_j$  and  $J_y$  have similar meanings. For  $I' \subseteq I$ , write

$$\bigcap_{i \in I'} X_i = X^*(I')$$

and

$$\bigcup_{1 \in I'} X_1 = X(I').$$

A similar convention holds for  $Y^*(J')$ , etc. Let  $\mathcal{F}$  denote the family of subsets  $J'$  of  $J$  for which

$$Y[J'] = Y^*(J') \setminus Y(J \setminus J')$$

is nonempty. These sets  $Y[J']$  are the boolean atoms generated by  $(Y_j: j \in J)$  (see p. 14 of [7]). The family  $(Y[J']: J' \in \mathcal{F})$  is a partition of  $Y$  into  $r$  nonempty subsets  $Y[J']$ , for some  $r \leq n$ .

We can state a result of Rado [9], which is analogous to P. Hall's Theorem, as follows:

Theorem 3 (Rado) Let  $G(I, X)$  and  $H(J, Y)$  be bipartite graphs with  $|I| = |J|$ ,  $|X| \geq |Y|$ . Let  $(X_1: 1 \in I)$  and  $(Y_j: j \in J)$  and  $\mathcal{F}$  be as defined above. Let  $\pi: J \rightarrow I$  be a bijection. A necessary and sufficient condition that there exist an injection  $\varphi: Y \rightarrow X$  such that  $\pi$  and  $\varphi$  define an embedding of  $H(J, Y)$  into  $G(I, X)$  is that for any nonempty subfamily  $\mathcal{F}'$  of  $\mathcal{F}$ ,

$$(2.1) \quad \left| \bigcup_{J' \in \mathcal{F}'} X^*(\pi J') \right| \geq \left| \bigcup_{J' \in \mathcal{F}'} Y^*(J') \right|.$$

Our statement of Rado's Theorem is more like the formulation in Mirsky's book [7] than the statement in Rado's paper. As stated in Mirsky's book,



however, (2.1) must hold for any family of subsets  $J'$  of  $J$ , not necessarily all in  $\mathcal{F}$ . However, since  $Y[J']$  is empty when  $J'$  is not in  $\mathcal{F}$ , it is easy to see from the proof in 7 that we only need to consider  $J' \in \mathcal{F}$ .

3. Subgraphs of bipartite graphs. It would be of interest to know a condition for a bipartite graph  $H(J,Y)$  to be a subgraph of another bipartite graph  $G(I,X)$ . Theorem 3 provides a means of extending, if possible, a bijection  $\pi: J \rightarrow I$  to an embedding of  $H(J,Y)$  into  $G(I,X)$ . We shall prove the following:

Theorem 4 Let  $G(I,X)$  and  $H(J,Y)$  be bipartite graphs with  $|I| = |J|$ ,  $|X| \geq |Y|$ , and let

$$(3.1) \quad d = \max_{v \in J \cup Y} \deg_{H(J,Y)}(v).$$

Let  $s$  and  $t$  be the real numbers satisfying

$$(3.2) \quad (1-s)|X| = \min_{i \in I} \deg_{G(I,X)}(i)$$

and

$$(3.3) \quad (1-t)|I| = \min_{x \in X} \deg_{G(I,X)}(x).$$

If also,

$$(3.4) \quad d(s|X| + t|I|) \leq |X|,$$

then  $H(J,Y)$  can be embedded into  $G(I,X)$ . Moreover, for any bijection  $\pi: J \rightarrow I$ , there is an injection  $\varphi: Y \rightarrow X$  such that  $\pi$  and  $\varphi$  define such an embedding.

Proof: It suffices to prove the latter conclusion, which implies the former. By Theorem 3, it suffices to prove (2.1) for any subfamily of  $\mathcal{F}$ .

By (3.1), for all  $j \in J$ ,

$$(3.5) \quad |Y_j| \leq d,$$

and for any  $y \in Y$ ,

$$(3.6) \quad |J_y| \leq d.$$

For any  $J' \in \mathcal{F}$ ,

$$(3.7) \quad |J'| \leq d,$$

by (3.6) and the definition of  $\mathcal{F}$ . Since  $J' \in \mathcal{F}$ ,  $Y[J']$  and  $Y^*(J')$  are nonempty.

Let  $\mathcal{F}'$  be a fixed subset of  $\mathcal{F}$ . Let  $R$  be a minimum subset of  $J$  such that  $R \cap J'$  is nonempty for all sets  $J'$  in  $\mathcal{F}'$ . Every point in  $\bigcup_{J' \in \mathcal{F}'} Y^*(J')$  lies in  $Y_j$  for some  $j \in R$ , so by (3.5),

$$(3.8) \quad \left| \bigcup_{J' \in \mathcal{F}'} Y^*(J') \right| \leq \left| \bigcup_{j \in R} Y_j \right| \leq |R| \max_j (|Y_j|) \leq |R|d.$$

Case I: Suppose

$$(3.9) \quad |R| > t|J|.$$

Assume that  $x \in X$  exists such that  $x \notin X^*(\pi J')$  for any  $J' \in \mathcal{F}'$ . By (3.3),

$$|I_x| \geq (1-t)|I|,$$

so

$$(3.10) \quad |I - I_x| \leq t|I|.$$

Now,  $x \notin X^*(\pi J')$  for any  $J' \in \mathcal{F}'$  implies that  $(I - I_x) \cap \pi J'$  is nonempty for any  $J' \in \mathcal{F}'$ . Since  $\pi$  is a bijection, this implies  $\pi^{-1}(I - I_x) \cap J'$  is

nonempty for any  $J' \in \mathcal{F}'$ . This is the property by which  $R$  is defined, so by (3.10),

$$|R| \leq |\pi^{-1}(I - I_X)| \leq t|I| = t|J|,$$

contradicting (3.9). Hence, the assumption

$x \notin X^*(\pi J')$  for any  $J' \in \mathcal{F}'$  is false and so  $x \in X^*(\pi J')$  for some  $J' \in \mathcal{F}'$ . Since  $x \in X$  is arbitrary,

$$|\bigcup_{\mathcal{F}'} X^*(\pi J')| = |X| \geq |Y| \geq |\bigcup_{\mathcal{F}'} Y^*(J')|,$$

proving (2.1) in this case.

Case II: Suppose

$$(3.11) \quad |R| \leq t|J|.$$

By (3.8) and (3.11),

$$(3.12) \quad |\bigcup_{\mathcal{F}'} Y^*(J')| \leq |R|d \leq td|J|.$$

Let  $J'' \in \mathcal{F}'$ . Then, by (3.6),  $X^*(\pi J'')$  is the intersection of  $|\pi J''| = |J''| \leq d$  sets  $X_1$  ( $1 \in \pi J''$ ), each covering all but at most  $s|X|$  vertices of  $X$ . Hence,  $X^*(\pi J'')$  covers all but at most  $sd|X|$  vertices of  $X$ . By the inequality (3.4) and by (3.12),

$$\begin{aligned} |\bigcup_{\mathcal{F}'} X^*(\pi J')| &\geq |X^*(\pi J'')| \geq |X| - sd|X| \\ &\geq td|I| = td|J| \geq |\bigcup_{\mathcal{F}'} Y^*(J')|, \end{aligned}$$

proving (2.1). Since (2.1) holds in either case, this theorem follows from Theorem 3.



Corollary Let  $G(I, X)$  and  $H(J, Y)$  be bipartite graphs with  $|I| = |J| = |X| \geq |Y|$ , and suppose that

$$d = \max_{v \in J \cup Y} \deg_{H(J, Y)}(v).$$

If

$$\frac{2d-1}{2d} |I| \leq \deg_{G(I, X)}(v)$$

for every vertex  $v \in I \cup X$ , then the conclusions of Theorem 4 hold.

Proof: The hypothesis of the corollary implies  $s, t \leq 1/2d$  in (3.2) and (3.3). Such values satisfy (3.4), so we can apply Theorem 4.

The minimum degree sequence required to obtain the conclusions of Theorem 4 may be relaxed a bit from the requirements of our result. However, in a certain sense, Theorem 4 is best possible.

Let  $I, X, d \geq 1$  be given. In showing that Theorem 4 is best possible, we may assume without loss of generality since  $s|X|$  is integral that  $(s, t)$  violates (3.4), but that  $(s - \frac{1}{|X|}, t)$  satisfies (3.4) when substituted for  $s$  and  $t$ . Using such values of  $s$  and  $t$ , we shall construct bipartite graphs  $G(I, X)$  and  $H(J, Y)$  satisfying (3.1), (3.2), and (3.3) but violating the conclusions of Theorem 4.

In our construction we assume that  $|X| = |Y|$  and

$$(3.13) \quad dt \leq 1.$$

This is not always true, but it is if  $|I| \geq |X|$  and  $s \neq 0$ . Then

$$s|X| \geq 1,$$

and if  $dt > 1$ , we obtain a contradiction:

$$d\left((s - \frac{1}{|X|})|X| + t|I|\right) \geq dt|I| > |I| \geq |X|.$$

If  $ds > 1$ , then  $ds$  exceeds 1 by a positive multiple of  $\frac{1}{|X|}$ , so

$$d(s - \frac{1}{|X|}) = ds - \frac{d}{|X|} \geq 1 + \frac{1-d}{|X|}.$$

Hence,

$$\begin{aligned} d(s - \frac{1}{|X|})|X| + dt|I| &\geq |X| + 1 - d + dt|I| \\ &\geq |X| + 1 > |X|, \end{aligned}$$

whence  $(s - \frac{1}{|X|}, t)$  violates (3.4), again contrary to our earlier assumption. Therefore,

$$(3.14) \quad ds \leq 1.$$

Let  $G(I, X)$  be a bipartite graph satisfying:

G1:  $V_1, V_2, \dots, V_d$  are subsets of  $X$  such that

$$(3.15) \quad |V_1| = (1-s)|X|$$

and

$$(3.16) \quad V_i \cup V_j = X$$

for any distinct  $i, j \leq d$ . Let  $V_0$  denote  $X$ .

G2:  $I$  is partitioned into sets  $W_0, W_1, \dots, W_d$ ,

with

$$(3.17) \quad |W_1| = |W_2| = \dots = |W_d| = t|I|.$$

G3: For  $i = 0, 1, \dots, d$ , each vertex of  $W_i$  is adjacent to every vertex of  $V_i$  and to no others.

First, we note that such a graph  $G(I, X)$  exists. By (3.14), both (3.15) and (3.16) hold for some choice of sets  $(V_i: i=1, \dots, d)$ , and by (3.13), (3.17) holds for some partition.

Note that  $W_1, W_2, \dots, W_d$  contain vertices of degree  $(1-s)|X|$ , by (G3) and (G1), and so (3.2) holds. A vertex of  $X \setminus V_j$  lies, by (3.16), in  $V_i$  for all  $i \neq j$ , so by (G3),  $x$  is adjacent to exactly those members of  $I$  not in  $W_j$ . Since their number, by (3.17), is  $(1-t)|I|$ , (3.3) holds. Vertices in  $W_0$  or  $V_1 \cap \dots \cap V_d$  are adjacent to all vertices on the opposite side of the bipartition. By inclusion and exclusion and (G1),

$$(3.18) \quad |V_1 \cap \dots \cap V_d| = |X| - sd|X|.$$

Let  $H(J, Y)$  be a graph of maximum degree  $d$  defined as follows: let  $|J| = |I|$ ,  $|Y| = |X|$ . Let  $(U_0, \dots, U_d)$  be a partition of  $J$  such that there is a bijection  $\pi: J \rightarrow I$  with

$$\pi(U_i) = W_i \quad (i = 0, 1, \dots, d).$$

Let the components of  $H(J, Y)$  include  $|W_1|$  components isomorphic to the complete bipartite graph  $K_{d,d}$  and each having a vertex in  $U_i$  for  $i = 1, 2, \dots, d$ . The

components induced by  $U_0$  and remaining vertices of  $Y$  may be any bipartite graph with degree at most  $d$ .

Thus, there is a set, say  $Y'$ , of

$|U_1| + \dots + |U_d|$  vertices  $y \in Y$  which are adjacent to a member of each of  $U_1, U_2, \dots, U_d$ . Hence, if  $\varphi$  exists as in Theorem 4, then  $\varphi(y)$  must be adjacent to a vertex of each of  $\pi(U_i) = W_i$  ( $i=1, \dots, d$ ) for all  $y \in Y'$ . This implies

$$(3.19) \quad \varphi(Y') \subseteq V_1 \cap \dots \cap V_d,$$

by (G3) and the fact that  $(W_i: i = 0, 1, \dots, d)$  is a partition. But

$$\begin{aligned} |Y'| &= \sum_{i=1}^d |U_i| = \sum_{i=1}^d |W_i| = td|I| \\ &> |X| - sd|X| = |V_1 \cap \dots \cap V_d| \end{aligned}$$

by (3.17), the fact that (3.4) is assumed violated, and (3.18). This contradicts (3.19), so  $\varphi$  cannot exist, and the conclusion of Theorem 4 cannot hold.



4. Subgraphs of simple graphs. In this section we consider the problem of giving a nontrivial sufficient condition for a graph to be embedded in another graph. We shall use Theorem 4 of the previous section.

Theorem 5 Let  $G$  and  $H$  be graphs on  $p$  vertices, and let  $d$  denote the maximum degree of vertices of  $H$ . If

$$(4.1) \quad \deg_G(v) \geq p \left( 1 - \frac{1}{2d(d+1)} \right) - 1$$

for every vertex  $v$  of  $G$ , then  $H$  can be embedded in  $G$ .

Proof: Let  $G$  and  $H$  be graphs satisfying the hypothesis of the theorem.

Denote  $H$  by  $H_d$ , and let  $S_d$  denote a maximal set of mutually nonadjacent vertices. Let  $T_d = V(H_d) \setminus S_d$ , and define  $H_{d-1} = H_d[T_d]$ , where  $H[W]$  denotes the subgraph of  $H$  generated by  $W \subseteq V(H)$ .

Recursively, let

$$(4.2) \quad H_{k-1} = H[T_k], \quad (k = d, d-1, \dots, m+1),$$

where

$$(4.3) \quad S_k = V(H_k) \setminus T_k \quad (k = d, d-1, \dots, m)$$

is a fixed maximal set of independent vertices of  $H_k$ , and where  $k = m$  is the largest integer for which  $H_k$  has no edges. Clearly,  $H_{d-1}, \dots, H_m$  are dependent upon the choice of  $S_d, \dots, S_{m+1}$ . However, since  $(S_k: k = m+1, \dots, d)$  is to be fixed throughout this proof, this presents no problem.

Since  $S_k$  is a maximal set of independent vertices of  $H_k$ ,

$$(4.4) \quad \deg_{H_k}(v) > \deg_{H_{k-1}}(v)$$

for all  $v \in V(H_{k-1})$ . Therefore,  $m \geq 0$  and

$$(4.5) \quad \deg_{H_k}(v) \leq k \quad (k = m, \dots, d).$$

We now prove

$$(4.6) \quad |V(H_k)| \leq |S_k|(k+1) \quad (k = m, \dots, d).$$

Each vertex of

$$T_k = V(H_k) \setminus S_k$$

is adjacent to a vertex of  $S_k$ . By (4.5), each vertex of  $S_k$  is adjacent to at most  $k$  vertices in  $H_k$ , whence

$$|T_k| \leq k|S_k|,$$

and so

$$|V(H_k)| = |T_k| + |S_k| \leq k|S_k| + |S_k|,$$

which proves (4.6).

Now by (4.2), (4.6), and (4.3), we have

$$\begin{aligned} |V(H_{k-1})| + |V(H_k)|/(k+1) &\leq |T_k| + |S_k| \\ &= |V(H_k)|. \end{aligned}$$

Therefore,

$$|V(H_{k-1})| \leq \frac{k}{k+1} |V(H_k)|,$$

whence

$$\begin{aligned} (4.7) \quad |V(H_k)| &\leq \frac{k+1}{k+2} \cdot \frac{k+2}{k+3} \cdots \frac{d}{d+1} |V(H_d)| \\ &= \frac{k+1}{d+1} p \quad (k = m, \dots, d). \end{aligned}$$

The graph  $H_m$ , having no edges, can be embedded in  $G$ . Let this be a basis for induction.

By the induction hypothesis, for  $k = m, \dots, d+1$ , there is an embedding  $\pi_k: V(H_k) \rightarrow V(G)$ . Define

$$I_k = \pi_k[V(H_k)],$$

and define

$$(4.8) \quad X_k = V(G) \setminus I_k.$$

Then (4.7) becomes

$$(4.9) \quad |X_k| = p - |V(H_k)| \geq p(1 - \frac{k+1}{d+1}) \\ = p \frac{d-k}{d+1} \quad (k = m, \dots, d-1).$$

Let  $G(I_k, X_k)$  denote the bipartite graph obtained from  $G$  by removing all edges not joining vertices of  $I_k$  and  $X_k$ . For all  $x \in X_k$ ,

$$\deg_{G(I_k, X_k)}(x) \geq \deg_G(x) - |X_k| + 1,$$

and for all  $i \in I_k$ ,

$$\deg_{G(I_k, X_k)}(i) \geq \deg_G(i) - |I_k| + 1.$$

Let  $s = s_k$  and  $t = t_k$  be the real numbers  $s, t$  of (3.2) and (3.3) for  $G(I_k, X_k)$ . Let  $i^*$  and  $x^*$  be members of  $I_k$  and  $X_k$ , respectively, for which the minima of (3.2) and (3.3) are attained for  $G(I_k, X_k)$ . We combine the above inequalities with (3.2), (3.3), and (4.8) to obtain

$$\begin{aligned}
 (4.10) \quad t|I_k| &= |I_k| - \deg_{G(I_k, X_k)}(x^*) \\
 &\leq |I_k| - \deg_G(x^*) + |X_k| - 1 \\
 &= p - \deg_G(x^*) - 1.
 \end{aligned}$$

$$(4.11) \quad s|X_k| \leq p - \deg_G(1^*) - 1.$$

Combining (4.10) and (4.11) with (4.1), (4.9), and  $m \geq 0$ , we get for  $k = m, \dots, d-1$ ,

$$\begin{aligned}
 (4.12) \quad (k+1)(s|X_k| + t|I_k|) \\
 &\leq (k+1)(2p - 2 - \deg_G(x^*) - \deg_G(1^*)) \\
 &= (k+1)\frac{p}{d(d+1)} \leq \frac{k+1}{d(d-k)}|X_k| \leq |X_k|.
 \end{aligned}$$

The maximum degree of  $H_{k+1}(V(H_k), V(H_{k+1}) \setminus V(H_k))$  is at most  $k+1$ , by (4.5). By the definition of  $I_k$ ,

$$(4.13) \quad |V(H_k)| = |I_k|.$$

By (4.8), (4.13) and  $|V(G)| = |V(H)| \geq |V(H_{k+1})|$ ,

$$|X_k| \geq |V(H_{k+1}) \setminus V(H_k)|.$$

Also, since (4.12) is simply (3.4) for  $G(I_k, X_k)$  and since (3.2) and (3.3) are valid in  $G(I_k, X_k)$ , we have satisfied the hypothesis of Theorem 4. Therefore, there is an injection  $\varphi_k: V(H_{k+1}) \setminus V(H_k) \rightarrow X_k$ , such that  $\pi_k$  and  $\varphi_k$  define an embedding of  $H_{k+1}(V(H_k), V(H_{k+1}) \setminus V(H_k))$  into  $G(I_k, X_k)$ . Now,  $\pi_k$  is already an embedding of  $H_k$  into  $G$ , and so  $\pi_k$  and  $\varphi_k$  define an embedding of  $H_{k+1}$  into  $G$ . The theorem follows by induction.



We now strengthen Theorem 5 for certain graphs with  $d = 2$ . A component of a graph is odd or even according as the number of its vertices is odd or even.

Theorem 6 Let  $G$  be a simple graph on  $p$  vertices,  $p$  even. Let  $H$  be a simple graph on  $p$  vertices of maximum degree 2. If the minimum degree of  $G$  is at least  $\frac{7}{8}p - 1$  and if the number  $k$  of odd polygons in  $H$  is not more than the number of nonpolygonal odd components, then  $H$  can be embedded in  $G$ .

Proof: It follows from the hypothesis that  $H$  consists of polygons, arcs, or isolated vertices. Let a maximum set  $Y_1$  of nonadjacent vertices be selected from the polygons of  $H$ . By hypothesis, we can take a set of  $k$  nonpolygonal odd components, and from these let a maximum set  $Y_2$  of nonadjacent vertices be chosen. Among the components thus considered, exactly half of their vertices lie in  $Y_1 \cup Y_2$ . Since  $p$  is even, the number of odd components is even, so there remain, if any, an even number of nonpolygonal odd components. Choose a set  $Y_3$  of independent vertices of these components, so that exactly half of the vertices of these components lie in  $Y_3$ . This

can be done by choosing a maximal independent edge cover for half of the remaining components and a minimal independent edge cover for the others. Let  $Y = Y_1 \cup Y_2 \cup Y_3$ , and let  $J = V(H) \setminus Y$ . Then

$$|Y| = |J| = p/2.$$

Let  $H(J, Y)$  be the bipartite graph obtained from  $H$  by deleting the one edge from each polygon that is not covered by  $Y_1$ . Since the minimum degree of vertices of  $G$  is large, we can choose a matching  $M$  in  $G$  of as many edges as there are edges removed from  $H$  to get  $H(J, Y)$ . Let  $I$  be an arbitrary set of  $|J|$  vertices of  $G$  containing the vertices covered by  $M$ . Let  $\pi: J \rightarrow I$  map vertices joined in  $H$  but not joined in  $H(J, Y)$  to vertices joined in  $M$ . Let  $X = V(G) \setminus I$ . Then

$$|I| = |J| = |X| = |Y| = p/2.$$

Since the minimum degree of  $G$  is at least  $\frac{7}{8}p - 1$ , the minimum degree of a vertex in  $G(I, X)$  is at least  $\frac{3}{8}p$ . Now,  $\frac{3}{8}p = \frac{2d-1}{2d}|I|$ , where  $d = 2$  and  $p = 2|I|$ , and so we can apply the Corollary to Theorem 4 and conclude that there exists a mapping  $\varphi: Y \rightarrow X$  such that  $\varphi$  and  $\pi$  define an embedding of  $H$  into  $G$ . This completes the proof.

5. The number of 1-factors of a graph. Anderson [1] and Gallai [4] used Theorem 1 (or its equivalent) to prove Tutte's Theorem [10] characterizing graphs having 1-factors. In this section we shall use Theorem 2 in a similar manner to obtain lower bounds on the number of 1-factors of a graph.

J. Zaks [12] substantially improved a lower bound of Beineke and Plummer [2] on the number of 1-factors of an  $n$ -connected graph. A graph on more than  $\max(2, n)$  vertices ( $n > 0$ ) is  $n$ -connected if the removal of fewer than  $n$  vertices does not separate the graph into several components. We shall improve these bounds.

Tutte's Theorem is stated in Theorem 7 below. Berge [3] has given a formula for the maximum number of independent edges in a graph. This can be derived from the defect version of P. Hall's Theorem (see [7], p. 40) using the method of Anderson [1]. Tutte [11] has used his theorem on 1-factors to prove a general factor theorem for arbitrary graphs.

The graph obtained by deleting a set  $S$  of vertices from the graph  $G$  is denoted  $G - S$ . The set of odd components of a graph  $G - S$ ,  $S \subseteq V(G)$  is denoted  $C_G(S)$  or, more simply,  $C(S)$ . Let  $f(G)$  denote

the number of 1-factors of  $G$ . It is easily seen that for any  $v \in V(G)$ ,

$$(5.1) \quad \sum_{\substack{w \in V(G) \\ w \text{ adj } v}} f(G - \{v, w\}) = f(G),$$

where the sum is over all vertices  $w \in V(G)$  adjacent to  $v$ . We state without proof Tutte's 1-factor Theorem [10]:

Theorem 7 (Tutte) A necessary and sufficient condition that  $f(G) > 0$  for a graph  $G$  is that for every set  $S \subseteq V(G)$ ,

$$|C(S)| \leq |S|.$$

We shall use the following result:

Theorem 8 Let  $G$  be an  $n$ -connected graph with  $f(G) \geq 1$ . Then

- (i) if  $|C(S)| = |S|$  for some  $S \subseteq V(G)$  whose removal disconnects  $G$ , then  $f(G) \geq n!$ ;
- (ii) if  $|C(S)| < |S|$  for all  $S \subseteq V(G)$  whose removal disconnects  $G$ , then  $f(G - \{v, w\}) \geq 1$  for all pairs of adjacent vertices  $v, w$ .

Outline of Proof: Anderson [1] shows that in case (i), Theorem 1 may be used to prove the existence of a set of edges joining  $S_0$  and  $C(S_0)$ , where  $S_0$  is a maximal disconnecting set for which

$$|C(S)| = |S|.$$



Furthermore, such a set of edges is contained in a 1-factor. Now, the assumption of  $n$ -connectedness permits the use of Theorem 2 in Anderson's proof. This implies that there are at least  $n!$  sets of edges joining  $S_0$  and  $C(S_0)$ , and each set is contained in a different 1-factor, whence (1).

Part (ii) is a routine result which does even use  $n$ -connectedness. Anderson [1] also covers this case in his proof of Tutte's Theorem.

If  $n < 4$ , define  $h(n) = n$ ; otherwise, if  $n > 4$ , let

$$h(n) = r(n) \prod_k (n-4k)(n-4k-1),$$

where the product is taken over all nonnegative integers  $k$  for which  $n - 4k - 1$  is positive, and where

$$r(n) = \begin{cases} 2/3 & \text{if } n \equiv 0 \pmod{4}; \\ 1 & \text{if } n \equiv 1 \text{ or } 2 \pmod{4}; \\ 1/2 & \text{if } n \equiv 3 \pmod{4}. \end{cases}$$

Thus, for  $n = 1, 2, \dots$ , we have  $h(n) = 1, 2, 3, 8, 20, 60, 126, 448, 1440, 5400$ , etc. In [12], J.

Zaks showed that if  $G$  is an  $n$ -connected graph, then

$$f(G) \geq n(n-2)(n-4)(n-6) \dots$$

We improve this for  $n > 4$  by proving the following:

Theorem 9 If  $G$  is any  $n$ -connected graph with a 1-factor and with at least  $n+2$  vertices, then

$$f(G) \geq h(n).$$

Proof: Let  $G$  be an  $n$ -connected graph with a 1-factor. By Theorem 7,  $|C(S)| \leq |S|$  for all  $S \subseteq V(G)$ . If  $|C(S)| = |S|$  for some set  $S \subseteq V(G)$  whose removal separates  $G$ , then  $f(G) \geq n!$ , by (1) of Theorem 8. Since  $n! \geq h(n)$  for all  $n$ , the theorem follows in this case. If  $|C(S)| < |S|$  for all  $S \subseteq V(G)$  whose removal separates  $G$ , then any edge of  $G$  is contained in a 1-factor. By the hypothesis of this theorem,  $G$  is not the complete graph on  $n+1$  vertices. Hence, we can find vertices  $v, v'$ , each adjacent to at least  $n$  vertices other than  $v$  or  $v'$ . Let  $w$  be one of those vertices adjacent to  $v$  and distinct from  $v'$ . The graph  $G - \{v, w\}$  either satisfies

$$|C_{G-\{v,w\}}(S)| = |S|$$

for some  $S \subseteq V(G)$ , in which case  $G - \{v, w\}$  has at least  $(n-2)!$  1-factors, or satisfies

$$|C_{G-\{v,w\}}(S)| < |S|$$

for all  $S \subseteq V(G)$  whose removal separates  $G - \{v, w\}$ , in which case all edges incident with the vertex  $v'$ , which has degree at least  $n-1$  in  $G - \{v, w\}$ , are part of 1-factors including the edge joining  $v$  and  $w$ .

In the former case,

$$f(G) \geq n(n-2)! \geq h(n);$$

in the latter case, by (11) of Theorem 8,

$$f(G) \geq n(n-1)f(G - \{v, w, v', w'\}),$$

where  $v, w$  and  $w', v'$  are endpoints of the first two edges of  $G$  chosen to be in a 1-factor. Since  $G - \{v, w, v', w'\}$  is  $(n-4)$ -connected, and is not a complete graph on  $n-3$  vertices, we can repeat this procedure and conclude inductively that

$$f(G) \geq n(n-1)(n-4)(n-5) \dots f(H),$$

where  $H$  is the subgraph obtained from  $G$  by removing  $4\left[\frac{n-1}{4}\right]$  vertices  $v, w, v', w', \dots$ , etc., so that  $H$  is not necessarily 5-connected, but may be only 1-, 2-, 3-, or 4-connected. In these four cases, Theorem 8 implies  $f(H)$  is at least 1, 2, 3, or  $8 = \min(4!, 4 \cdot 2)$ , respectively; i.e.,

$$f(H) \geq r(n)(n - 4k)(n - 4k - 1)$$

for  $k = \left[\frac{n-1}{4}\right]$ , unless  $n \equiv 1 \pmod{4}$ , in which case

$$f(H) \geq r(n) = 1.$$

Combining these relations on  $f(H)$  with the definition of  $h(n)$ , we obtain  $f(G) \geq h(n)$ , proving the theorem.

The party graph (see [12], p. 487) is a graph for which the bound of Theorem 9 is attained when  $n=2, 4$ , or 6. These appear to be the only values of  $n \geq 1$  for which the result is best possible.

Theorem 9 can be slightly improved when  $n$  is large or when more exceptional graphs are excluded. These improvements are only of minor significance. Zaks [12] gives a discussion and some conjectures concerning such lower bounds.

Zaks [12] conjectured that if  $|V(G)| \geq 2n$ , and if  $G$  is an  $n$ -connected graph with a 1-factor, then  $f(G) \geq n!$ . This is false for the graph pictured in Figure 1. Figure 1 is a 3-connected graph with only five 1-factors, and  $|V(G)| = 2n+2 = 8$ . It does appear reasonable to conjecture, however, that for any given  $n$ ,  $f(G) \geq n!$  for all but finitely many graphs  $G$  that are  $n$ -connected and have a 1-factor. Even the case  $n = 3$  does not appear to be simple. Instead of  $n!$ , however, we can give the weaker bound of the following theorem. For  $n = 4, 5, 6, \dots$ , the bound given below is 8, 25, 72, 294, 1024, 4374, etc., an improvement over Theorem 9 when  $n > 4$ .

Theorem 10 For any natural number  $n \geq 3$ , let  $m$  be the largest integer having the same parity as  $n$  and satisfying  $m(m-1) < n$ . There are at most finitely many  $n$ -connected graphs  $G$  which have 1-factors and satisfy

$$f(G) < m! n^{\frac{1}{2}(n-m)}.$$



Proof: If  $G$  has a vertex  $v$  of degree at least  $n!$  and (11) of Theorem 8 holds, then  $G - \{v, w\}$  has a 1-factor for  $n!$  values of  $w$ , where  $w$  is adjacent to  $v$ , determining at least  $n!$  different 1-factors. If (1) holds, then  $G$  has  $n!$  different 1-factors, since  $G$  is  $n$ -connected and has a 1-factor. Since

$$n! \geq m! n^{\frac{1}{2}(n-m)},$$

it suffices to restrict our attention to graphs  $G$  in which all vertices have degree less than  $n!$  and for which (11) of Theorem 8 holds.

By this restriction, the number of vertices having distance 2 from  $v$  is at most  $(n! - 1)^2$ , so the number of vertices within distance 0, 1, 2 of  $v$  is less than  $n!^2$ . It follows that if  $G$  has  $\left[\frac{n}{2}\right](n!)^2$  or more vertices, then there are  $\left[\frac{n}{2}\right]$  vertices  $V = \{v_1, v_2, \dots, v_{\left[\frac{n}{2}\right]}\}$ , no two separated by distance 2 or less. (The brackets denote the greatest integer function). We only exclude finitely many graphs by assuming that  $G$  has at least  $\left[\frac{n}{2}\right]n!^2$  vertices, and so we can prove the theorem by showing that such graphs have at least  $m! n^{\frac{1}{2}(n-m)}$  1-factors.

We now show that for some  $k \leq \left[\frac{n}{2}\right]$ ,

$$(5.2) \quad f(G) \geq n^k(n-2k)!$$

Let  $H_0 = G$  and

$$H_k = G - \bigcup_{i=1}^k \{v_i, w_i\}.$$

where  $w_1$  is a vertex adjacent to  $v_1$  that minimizes  $f(H_{1-1} - \{v_1, w_1\})$ . As a basis for induction on  $k$ , observe that  $H_0$  is an  $n$ -connected graph with

$$f(G) \geq n^0 f(H_0).$$

Suppose  $H_k$  is an  $(n-2k)$ -connected graph with a 1-factor, and suppose that

$$k \leq \lfloor n/2 \rfloor - 1$$

and

$$f(G) \geq n^k f(H_k).$$

If  $H_k$  satisfies (i) of Theorem 8, then (5.2) is satisfied. Otherwise,  $H_k$  satisfies (ii). Since  $v_{k+1}$  is not within distance 2 of  $v_1$  ( $1 \leq k$ ), and not within distance 1 of  $w_1$  ( $1 \leq k$ ),

$$\deg_{H_k}(v_{k+1}) = \deg_G(v_{k+1}) \geq n.$$

Thus, by (ii) of Theorem 8,

$$\begin{aligned} f(G) &\geq n^k (\deg_{H_k}(v_{k+1})) \min_{w \text{ adj } v_{k+1}} f(H_k - \{v_{k+1}, w\}) \\ &\geq n^{k+1} f(H_k - \{v_{k+1}, w_{k+1}\}) \\ &= n^{k+1} f(H_{k+1}), \end{aligned}$$

and if  $2(k+1) < n$ , then  $H_{k+1}$  is  $(n-2(k+1))$ -connected.

Thus, by induction, either (5.2) follows for some

$k < \lfloor n/2 \rfloor$ , or

$$f(G) \geq n^{\lfloor n/2 \rfloor} f(H_{\lfloor n/2 \rfloor}).$$

In the latter case, since  $H_{[n/2]}$  has a 1-factor,

$$f(H_{[n/2]}) \geq (n-2[n/2])!,$$

whence

$$f(G) \geq n^{[n/2]} (n-2[n/2])!,$$

which implies (5.2).

The least value of  $n^k(n-2k)!$  for  $k \leq [n/2]$  is attained when  $n - 2k = m$ , where  $m$  is the integer defined in the statement of the theorem: for if  $k$  is increased from at least  $\frac{1}{2}(n-m)$ , then the factor  $n^k$  is multiplied by  $n$ , and  $(n-2k)!$  is divided by  $(n-2k)(n-2k-1)$ , which is less than  $m(m-1)$  and thus less than  $n$ , by the definition of  $m$ ; if  $k$  is decreased from  $\frac{1}{2}(n-m)$  or less, then  $n^k$  is divided by  $n$ , and  $(n-2k)!$  is multiplied by  $(n-2k)(n-2k-1)$ , which is at least  $(m+1)m$  and hence at least  $n$ . Therefore, by (5.2),

$$f(G) > m! n^{\frac{1}{2}(n-m)},$$

so the theorem is proved.

6. The 2-factors of graphs. Petersen [8]

showed that a graph is 2-factorable (i.e., is the union of edge-disjoint 2-factors) if and only if it is regular of even degree. It is known that this follows from P. Hall's Theorem. We shall generalize this using Theorem 1, showing that a graph of even degree that is "almost" regular also has many disjoint 2-factors. Also, we give a lower bound on the number of 2-factors of a graph. Tutte's Factor Theorem [11] gives a criterion for an arbitrary graph to have a 2-factor.

We define a graph  $G$  to be almost regular of degree  $2n$  if  $d < n$ , where

$$(6.1) \quad d = \frac{1}{2} \sum_{v \in V(G)} |\deg_G(v) - 2n|.$$

The number  $d$  is called the regularity defect of  $G$ . If  $d = 0$ ,  $G$  is regular of degree  $2n$ .

A graph is eulerian if there is a closed walk (called an eulerian walk) in  $G$  that traverses each edge of  $G$  exactly once. Euler showed, and it is well known, that a graph is eulerian if and only if it is connected and each of its vertices has even degree. A 2-factor is said to be compatible with an eulerian walk  $W$  of  $G$  if  $W$  restricted to any polygon of the 2-factor is also an eulerian walk.



Theorem 11 Let  $G$  be an eulerian graph that is almost regular of degree  $2n$  with regularity defect  $d \leq n$ . Then  $G$  has a 2-factor compatible with any of its eulerian walks. Any 2-factor is in a set of  $n - d$  edge disjoint 2-factors.

Proof: Given an eulerian walk of  $G$ , let  $A_v$  denote the set of vertices of  $G$  that immediately follow an occurrence of  $v \in V(G)$  in the walk. For any  $V \subseteq V(G)$ , let  $A(V)$  denote  $\bigcup_{v \in V} A_v$ . Let  $G'$  denote the directed graph obtained from  $G$  by directing each edge in the direction of the walk. Let  $V$  be an arbitrary subset of  $V(G)$ . We first prove

$$(6.2) \quad |V| \leq |A(V)|.$$

Let  $E$  denote the set of edges  $e$  of  $G'$  for which there is a vertex  $v \in V$  such that  $e$  is directed away from the vertex  $v$ ; let  $E'$  denote the set of edges  $e$  for which there is a vertex  $v \in A(V)$  such that  $e$  is directed toward the vertex  $v$ . Since an eulerian walk enters a vertex as many times as it leaves, the number of edges of  $E$  (or  $E'$ ) incident with a given vertex  $v \in V$  (or  $\in A(V)$ , resp.) is  $\frac{1}{2} \deg_G(v)$ . Hence,

$$\begin{aligned} (6.3) \quad |E| &= \frac{1}{2} \sum_{v \in V} \deg_G(v) \\ &= n|V| + \frac{1}{2} \sum_{v \in V} (\deg_G(v) - 2n), \end{aligned}$$

and similarly,

$$(6.4) \quad |E'| = n|A(V)| + \frac{1}{2} \sum_{w \in A(V)} (\deg_G(w) - 2n).$$

By the definition of  $A$ ,  $E \subseteq E'$ , whence

$$(6.5) \quad |E| \leq |E'|.$$

Combining (6.3), (6.4), (6.5), and (6.1), we get

$$\begin{aligned} n|V| &\leq n|A(V)| + \sum_{w \in A(V) \setminus V} (\deg_G(w) - 2n) \\ &\quad - \sum_{v \in V \setminus A(V)} (\deg_G(v) - 2n) \\ &\leq n|A(V)| + d \\ &< n|A(V)| + n. \end{aligned}$$

Therefore,

$$|V| < |A(V)| + 1,$$

and since  $|V|$  and  $|A(V)|$  are integers, this gives (6.2).

By (6.2), we can use Theorem 1 and conclude that  $(A_v: v \in V(G))$  has an SDR  $(x(v): v \in V(G))$ . The spanning subgraph consisting of the edges of  $G$  joining  $v$  and  $x(v)$  for some  $v \in V(G)$  is a 2-factor of  $G$ . This proves the first part of the theorem. The removal of the edges of the 2-factor from  $G$  leaves a graph, say  $G_1$ , with regularity defect  $d$  that is almost regular if  $n-1 > d$ . Suppose inductively, that Theorem 11 holds for graphs that are almost regular of degree  $2n-2$ . Then  $G_1$  has  $n-1-d$  edge-disjoint 2-factors, and these together with our 2-factor of  $G$  define a set of  $n-d$  edge-disjoint 2-factors of  $G$ . A basis for induction is easy to establish, so the theorem is proved.

Not all 2-factors are compatible with a given walk, so the following theorem only gives a lower bound on the number of 2-factors having the specific property of compatibility.

Theorem 12 Let  $G$  be a graph having a 2-factor. If the minimum degree of  $G$  is  $2m$  or  $2m+1$ , then  $G$  has at least  $m!$  2-factors.

Proof: Find the polygons of  $G$  that form a 2-factor and direct their edges so that no vertex of any polygon has two incoming edges or two outgoing edges. We claim that the remaining edges of  $G$  can be directed so that the number of incoming edges at any vertex is within one of the number of outgoing edges: simply find edge-disjoint polygons, direct their edges so that each vertex has as many incoming as outgoing edges; the remaining edges form a tree and can be partitioned into paths, no two having a common endpoint. Direct each edge of a path in the same direction along the path.

Now, define  $A_v$  as in the proof of Theorem 11. Observe that since  $G$  has a 2-factor,

$$|A(v)| \geq |v|$$

for all  $v \in V(G)$ . By our method of assigning direc-

tions to edges,  $|A_v| \geq m$  for all  $v$ . Therefore, since  $m \leq |V(G)|$ , we can apply Theorem 2 and conclude that the family of sets  $(A_v: v \in V(G))$  has at least  $m!$  SDR's, and each SDR determines a different 2-factor compatible with the directed graph, as in Theorem 12. This completes the proof.



## REFERENCES

1. I. Anderson, Perfect matchings of a graph, J. Combinatorial Theory 10(1971), 183-186.
2. L. Beineke and M. Plummer, On the 1-factors of a non-separable graph. J. Combinatorial Theory 2(1967), 285-289.
3. C. Berge, Sur le couplage maximum d'un graphe. C. R. Acad. Sci. Paris 247(1958), 258-259.
4. T. Gallai, Neuer Beweis eines Tutte'schen Satzes. Magyar Tud. Akad. Mat. Kutato Int. Kozl. 8(1963), 135-139.
5. M. Hall, Distinct representatives of subsets. Bull. Amer. Math. Soc. 51(1948), 922-926.
6. P. Hall, On representatives of subsets. J. London Math. Soc. 10(1935), 26-30.
7. L. Mirsky, Transversal Theory. Math. in Sci. and Eng., vol. 75 (1971) Academic Press.
8. J. Petersen, Die Theorie der regulären Graphen. Acta Math. 15(1891), 193-200.
9. R. Rado, A theorem on general measure functions. Proc. London Math. Soc. 22(1947), 107-111.
10. W. Tutte, The factorization of linear graphs. J. London Math. Soc. 22(1947), 107-111.
11. ———, A short proof of the factor theorem for finite graphs. Canad. J. Math. 6(1954), 347-352.
12. J. Zaks, On the 1-factors of n-connected graphs. Comb. Struct. and Their Applic., Proc. Calgary Inter. Conf., 481-488.

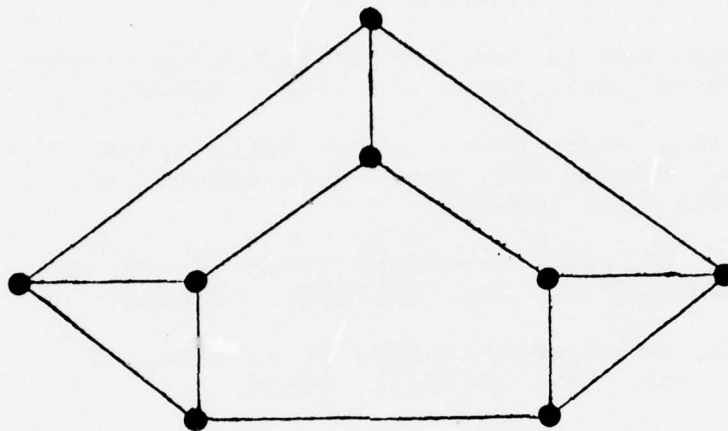


Figure 1

A 3-connected graph with five 1-factors.

APPENDIX II

UPPER AND LOWER BOUNDS  
FOR  
UNRESTRICTED BINARY ERROR CORRECTING CODES

A Thesis

Presented in Partial Fulfillment of the Requirements  
for the Degree Master of Science

by

Michael Ellis Segal, B.S.

The Ohio State University

1973

Approved by

\_\_\_\_\_  
Advisor  
Department of Mathematics

### Acknowledgements

The author especially wishes to thank Professor R. M. Wilson for his advice, encouragement and invaluable assistance. He also wishes to thank Professor A. E. Ross for his encouragement and continuing support and Professor D. K. Ray-Chaudhuri for his helpful comments.

This work was supported in part by ONR Contract N00014-67-A-0232-0016.



## TABLE OF CONTENTS

Acknowledgement	11
I. Introduction	
1. The Coding Problem	1
2. Definitions and Preliminary Ideas	3
3. Some Elementary Observations	8
II. The Function $A(n,d)$	
4. Some Elementary Observations on the Function $A(n,d)$	13
5. Some Bounds on $A(n,d)$	17
III. Construction of Codes	
6. Linear Codes and Hamming Codes	21
7. Cyclic Codes and Codes Based on Groups	31
8. Polynomial Codes, BCH Codes and RM Codes	37
9. A Class of Nonlinear Codes Derived from Polynomials	46
10. Constructions Using Hadamard Matrices, Conference Matrices and Combinatorial Designs	48
11. Refinements in Code Concatenation	53
12. Other Constructions for Combining Codes	60
IV. The Packing Problem and Refined Upper Bounds	
13. Johnson's Approach to the Packing Problem	65
14. Inequalities Involving Weight Distributions of Codewords	73
V. Collected Results	
15. An Exemplary Result on Weight Distribution	76
16. A Table of the Best Known Bounds for $A(n,d)$	79
References	91

## I. INTRODUCTION

### 1. The Coding Problem

The need for error correcting codes arises when considering those problems in data communications systems related to the transmission of a message across a channel. A channel is a device capable of transmitting the symbols which compose the message. The symbols presented to the channel are called input, and those received at the other end of the channel are called output. In an ideal communications system, the message is received exactly as it was transmitted, but transmission errors are quite common in practice. A channel is said to be noisy if an output symbol is not always the same as the corresponding input symbol.

Given a channel that is subject to noise, we consider the problem of making our communications system as error free as possible. One solution is the use of codes which are capable of detecting and/or correcting those errors that occur in transmission. To be practical, there should also be a reasonable method for encoding and decoding messages. The selection of the code and procedures for its encoding and decoding constitutes The Coding Problem.

This paper will be concerned with determining the maximum number of messages possible for codes of specific length; i.e. codes whose messages are composed of a specific number of symbols. We will limit our considerations to unrestricted (linear and nonlinear) binary codes (codes whose messages are composed of zeros and ones) and present a survey of known results. We will conclude with a table listing bounds on the maximum number of codewords for codes of length up to 50.

Remark. In addition to those cited at the end of this work, extensive lists of references may be found in Peterson and Weldon [18] and in Sloane [23].

## 2. Definitions and Preliminary Ideas

A vector (or word) of length  $n$  is a sequence of  $n$  symbols (i.e. an  $n$ -tuple) taken from a fixed set of elements called the alphabet. For example, we could consider the vector  $\underline{a} = (a_1, a_2, \dots, a_n)$ , where the  $a_i$  are elements of our alphabet. We note that if there are  $q$  elements in the alphabet, then there are  $q^n$  possible vectors. Since we are concerned only with binary codes, where the alphabet is  $Z_2$ , there are  $2^n$  possible vectors that could be used in a code of length  $n$ . We will denote by  $V_n$  the set of all possible  $n$ -tuples of elements of  $Z_2$ . For brevity, we will often denote  $\underline{a} = (a_1, a_2, \dots, a_n)$  by  $\underline{a} = a_1 a_2 \dots a_n$  or  $\underline{a} = (a_1 a_2 \dots a_n)$ .

If there were no noise in the channel, we could use all  $2^n$  possible vectors in transmission. One solution to the problem of noise is to select for transmission only some of the  $2^n$  possible sequences, choosing them to be sufficiently different so that if only a few transmission errors occur, the correct string may be found by comparing the received word with the set of reserved words. The subset of  $V_n$  selected for transmission is called a code of length  $n$ , which will be denoted by  $C$ . An element of a code will be called a codeword, to be distinguished from a general element of  $V_n$ , which will simply be called a vector.

Consider the set of all sequences of length  $k$  whose symbols are elements of  $Z_2$ . As we have noted, there are  $2^k$  of them, each providing a distinct message which may be used in transmission. Given these  $2^k$  vectors, we can develop a code by appending to each of them a vector of length  $r$ , for some  $r$ , where these  $r$  symbols from  $Z_2$  are determined in some way from the initial  $k$  symbols. This method gives us a vector



of length  $n = k + r$ , in which the first  $k$  symbols are called information digits and the remaining  $r$  symbols are called check digits. Such a vector is called a codeword of length  $n$ . This type of code, in which the codewords consist of  $k$  information digits and  $(n-k)$  check digits determined by them, is called a systematic code of dimension  $k$ . We note that to be systematic the  $k$  information digits need not be in the first  $k$  positions, but that the remaining  $(n-k)$  coordinates must be determined by them. We also remark that since each of our  $2^k$  vectors provides us with a distinct codeword, there are  $2^k$  codewords.

Let us consider a general alphabet  $T$  and suppose that the elements of  $T$  form an additive abelian group  $G$ . Then  $G^n = G \times G \times \dots \times G$  ( $n$  factors) is also a group under coordinatewise addition. A group code  $C$  with block length  $n$  and alphabet  $G$  is a subset of  $G^n$  which is also a subgroup. The weight  $w(a)$  of a vector in  $G^n$  is the number of nonzero coordinates. Furthermore, if the elements of our general alphabet  $T$  form a field  $F$ , then  $F^n$  may be viewed as a vector space of dimension  $n$  over the field  $F$ . A linear code  $C$  with block length  $n$  and alphabet  $F$  is a subset of  $F^n$  which is also a subspace of  $F^n$ .

**Remark.** A linear code is necessarily also a group code. In the case under consideration, where our alphabet is  $Z_2$ , every group code is also a linear code; i.e. the terms are synonymous for binary codes.

Given two vectors  $\underline{a}, \underline{b}$  of  $V_n$ , the Hamming distance  $\Delta(\underline{a}, \underline{b})$  is defined as the number of positions (or coordinates) in which  $\underline{a}$  and  $\underline{b}$  differ. If  $\underline{a} = (a_1, a_2, \dots, a_n)$  and  $\underline{b} = (b_1, b_2, \dots, b_n)$ , then  $\Delta(\underline{a}, \underline{b}) = |\{i : a_i \neq b_i\}|$ . For example, if  $\underline{a} = (1, 0, 0, 1)$  and  $\underline{b} = (0, 1, 0, 1)$ , then  $\Delta(\underline{a}, \underline{b}) = 2$  since they differ in the first and second coordinates.

For  $\underline{a}, \underline{b}$  of  $V_n$ , let  $\underline{a} \oplus \underline{b}$  denote the binary sum defined by coordinatewise addition modulo two; i.e.  $\underline{a} \oplus \underline{b} = (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n)$  for  $\underline{a} = (a_1, a_2, \dots, a_n)$ ,  $\underline{b} = (b_1, b_2, \dots, b_n)$ . For example, if  $\underline{a} = (0, 1, 1, 0)$  and  $\underline{b} = (1, 0, 1, 0)$ , then  $\underline{a} \oplus \underline{b} = (0 + 1, 1 + 0, 1 + 1, 0 + 0) = (1, 1, 0, 0)$ . We will often write  $\underline{a} \oplus \underline{b}$  simply as  $\underline{a} + \underline{b}$ . Note that the elements  $a_i + b_i$  are also elements of  $Z_2$ .

Proposition 2.1. Given  $\underline{a}, \underline{b}$  of  $V_n$ ,  $w(\underline{a} + \underline{b}) = \Delta(\underline{a}, \underline{b})$ .

Proof. Since addition is coordinatewise and since  $a_i + b_i = 0$  in  $Z_2$  whenever  $a_i = b_i$ , the weight of  $\underline{a} + \underline{b} = (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n)$  will be the number of coordinates in which  $\underline{a}$  and  $\underline{b}$  differ, or simply  $\Delta(\underline{a}, \underline{b})$ . QED

Proposition 2.2. The mapping  $\Delta: V_n \times V_n \rightarrow \{0, 1, \dots, n\}$  is a metric on  $V_n$ ; i.e. it satisfies the following properties for any  $\underline{a}, \underline{b}, \underline{c}$  of  $V_n$ :

- (i)  $\Delta(\underline{a}, \underline{b}) \geq 0$  and  $\Delta(\underline{a}, \underline{b}) = 0$  iff  $\underline{a} = \underline{b}$ ,
- (ii)  $\Delta(\underline{a}, \underline{b}) = \Delta(\underline{b}, \underline{a})$ ,
- (iii)  $\Delta(\underline{a}, \underline{b}) \leq \Delta(\underline{a}, \underline{c}) + \Delta(\underline{c}, \underline{b})$ .

Proof. Both (i) and (ii) are immediate from the definition of  $\Delta$ . From the properties of coordinatewise binary addition, clearly  $w(\underline{a} + \underline{b}) \leq w(\underline{a}) + w(\underline{b})$ . Then using Proposition 2.1, (iii) follows from  $\Delta(\underline{a}, \underline{b}) = w(\underline{a} + \underline{b}) = w(\underline{a} + \underline{c} + \underline{c} + \underline{b}) \leq w(\underline{a} + \underline{c}) + w(\underline{c} + \underline{b}) = \Delta(\underline{a}, \underline{c}) + \Delta(\underline{c}, \underline{b})$ . QED

Given a code  $C$ , we define  $d(C)$  to be the minimum distance between codewords of  $C$ ; i.e.  $d(C) = \min \Delta(\underline{a}, \underline{b})$  for distinct  $\underline{a}, \underline{b}$  of  $C$ .

Proposition 2.3. If  $C$  is a group code, then  $d(C) = \min w(\underline{a})$  for nonzero  $\underline{a}$  of  $C$ ; i.e. the minimum distance between codewords of  $C$  is the weight of the codeword of least nonzero weight.

Proof. If  $\underline{a}$  and  $\underline{b}$  are codewords, then  $\underline{a} + \underline{b}$  is a codeword since  $C$  is a group code. By Proposition 2.1, the distance between any two codewords is the weight of the codeword given by their sum. Since  $C$  is a group code, the null vector  $\underline{0}$  is a codeword, and the weight of any codeword  $\underline{a}$  is the distance between  $\underline{a}$  and  $\underline{0}$ . QED

By an  $(n,d)$ -code  $C$  we mean a code of length  $n$  such that the minimum distance between codewords is at least  $d$ . In other words,  $d(C) \geq d$ . We further denote by  $(n,d;A)$ -code a code of length  $n$ , minimum distance at least  $d$ , with  $A$  codewords. An  $(n,d)$ -code  $C$  is called optimal if no other  $(n,d)$ -code has more codewords than  $C$ . We denote by  $A(n,d)$  the number of codewords in an optimal  $(n,d)$ -code. It is the concern of this paper to discuss both upper and lower bounds on  $A(n,d)$ .

Example 2.4. Consider the code  $C$  given by the following vectors: 000000, 111000, 100110, 011110, 010101, 101101, 110011, 001011. This code can be verified to be a group code consisting of eight codewords of length six. Since  $C$  is a group code and since the minimum weight of its nonzero codewords is three, then by Proposition 2.3 we know that  $C$  is an  $(6,3;8)$ -code. This result proves that  $A(6,3) \geq 8$ . It will be proved in Section 4 that  $A(6,3) \leq 8$ , giving  $A(6,3) = 8$ .

Example 2.5. Consider the code  $C$  given by the vectors 00000, 11100, 00111, 11011. This is also a group code of length five with minimum distance of three between codewords. Then  $C$  is an  $(5,3;4)$ -code, proving

that  $A(5,3) \geq 4$ .

Remark. As we have observed, lower bounds on  $A(n,d)$  are generally found by construction; i.e. to prove  $A(n,d) \geq M$ , we produce an  $(n,d)$ -code with  $M$  elements. We also note that upper bounds are always determined by theoretical arguments.

We define another term often useful in the discussion of codes. For every vector  $\underline{a}$  of  $V_n$ , we define its complement  $\underline{a}'$  by  $\underline{a}' = \underline{a} + \underline{I}$ , where  $\underline{I}$  is the vector with ones in all positions. Thus the complement  $\underline{a}'$  of  $\underline{a}$  is obtained simply by interchanging zeros and ones in each coordinate. For example, the complement of 1001 is  $1001 + 1111 = 0110$ .



### 3. Some Elementary Observations

This section contains various results which are useful in studying  $A(n,d)$ , even though they are not directly related to each other.

A code is said to be e-error-detecting if it can detect as many as  $e$  errors. Similarly, a code is said to be e-error-correcting if it can correct up to  $e$  errors.

Proposition 3.1. Given a code  $C$ , then  $C$  is  $e$ -error-detecting if  $C$  is an  $(n, e + 1)$ -code and  $C$  is  $e$ -error-correcting if  $C$  is an  $(n, 2e + 1)$ -code.

Proof. If up to  $e$  errors occur in the transmission of a codeword of an  $(n, e + 1)$ -code, then the fact that the minimum distance between codewords is  $e + 1$  will ensure that the received vector will not be another codeword and error detection will result. In this case, nothing can be said about the originally transmitted codeword.

If up to  $e$  errors occur in the transmission of an  $(n, 2e + 1)$ -code, then since the minimum distance between codewords is  $2e + 1$ , the received vector will have a unique closest codeword which can be taken as the originally transmitted codeword. Thus error correction can occur. QED

Given a code  $C$  of length  $n$  and any vector  $\underline{a}$  of  $V_n$ , then the translate of  $C$  by  $\underline{a}$ , denoted by  $C_{\underline{a}}$ , is defined by  $C_{\underline{a}} = \{\underline{a} + \underline{b} : \underline{b} \in C\}$ .  $C_{\underline{a}}$  is the image of  $C$  under the mapping  $T_{\underline{a}} : V_n \rightarrow V_n$  as defined in

Proposition 3.2. The mapping  $T_{\underline{a}} : V_n \rightarrow V_n$  defined by  $\underline{b} \mapsto \underline{a} + \underline{b}$  is

distance preserving.

Proof. To show that  $T_{\underline{a}}$  preserves distance, we must show that  $\Delta(\underline{b}, \underline{c}) = \Delta(\underline{a} + \underline{b}, \underline{a} + \underline{c})$ . From Proposition 2.1 we have  $\Delta(\underline{a} + \underline{b}, \underline{a} + \underline{c}) = w(\underline{a} + \underline{b} + \underline{a} + \underline{c}) = w(\underline{b} + \underline{c}) = \Delta(\underline{b}, \underline{c})$ . QED

From the preceding proposition, we have immediately

Proposition 3.3. A translate of an  $(n, d)$ -code is also an  $(n, d)$ -code.

Given a code  $C$  of length  $n$  and a permutation  $P$  of  $\{1, 2, \dots, n\}$ , the permutation of  $C$  by  $P$ , denoted by  $C_P$ , is defined as  $C_P = \{(a_{P(1)}, a_{P(2)}, \dots, a_{P(n)}) : (a_1, a_2, \dots, a_n) \in C\}$ . We may also consider  $P$  as a mapping from  $V_n$  to  $V_n$  where  $\underline{a} \mapsto \underline{a}^P$ .

Proposition 3.4. The permutation  $P : V_n \rightarrow V_n$  defined by  $\underline{a} \mapsto \underline{a}^P$  is distance preserving.

Proof. To show that the permutation of a code preserves distance, we must show that  $\Delta(\underline{a}, \underline{b}) = \Delta(\underline{a}^P, \underline{b}^P)$ . Let  $\underline{a} = (a_1, a_2, \dots, a_n)$  and  $\underline{b} = (b_1, b_2, \dots, b_n)$ . Then for any  $i$ ,  $1 \leq i \leq n$ , consider the  $i^{\text{th}}$  coordinates of  $\underline{a}^P$  and  $\underline{b}^P$ , namely  $a_{P(i)}$  and  $b_{P(i)}$ . Then these coordinates will be the same or different according as the  $i^{\text{th}}$  coordinates of  $\underline{a}$  and  $\underline{b}$  are the same or different. But then  $\Delta(\underline{a}, \underline{b}) = \Delta(\underline{a}^P, \underline{b}^P)$  and the result follows. QED

From this result, we have immediately

Proposition 3.5. The permutation of an  $(n, d)$ -code produces an  $(n, d)$ -code.

We define two  $(n,d)$ -codes to be equivalent if you can obtain one from the other by means of a combination of translations and permutations. In terms of codewords, given two equivalent  $(n,d)$ -codes  $C_1$  and  $C_2$ , then for  $\underline{c} \in C_1$  we can determine its corresponding codeword in  $C_2$  by  $\underline{c} \mapsto \underline{c}^P + \underline{a}$  for some permutation  $P$  followed by a translation by some  $\underline{a}$  of  $V_n$ . The concept of equivalence will again be considered in the section on linear codes.

The vector  $\underline{a}$  is said to have even parity if  $w(\underline{a})$  is an even number, and odd parity if  $w(\underline{a})$  is an odd number. For example, the vector  $\underline{a} = (01111)$  has even parity and the vector  $\underline{b} = (01101)$  has odd parity since  $w(\underline{a}) = 4$  and  $w(\underline{b}) = 3$ .

Proposition 3.6. Let  $\underline{a}, \underline{b}$  be vectors of  $V_n$ . Then if  $\underline{a}$  and  $\underline{b}$  are of the same parity,  $\Delta(\underline{a}, \underline{b}) = 2k$  for some integer  $k$ . Similarly, if  $\underline{a}$  and  $\underline{b}$  are of different parity, then  $\Delta(\underline{a}, \underline{b}) = 2k + 1$ .

Proof. We can easily verify the equation  $w(\underline{a}) + w(\underline{b}) = 2c(\underline{a}, \underline{b}) + \Delta(\underline{a}, \underline{b})$ , where  $c(\underline{a}, \underline{b})$  is the number of coordinates in which  $\underline{a}$  and  $\underline{b}$  both have ones. The result follows trivially. QED

We next present several other results useful in later calculations for  $A(n,d)$ . Recalling that  $\binom{n}{k}$  is the number of ways of choosing  $k$  things from a set of  $n$  things, consider

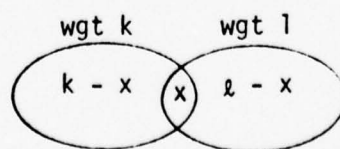
- Proposition 3.7.
- (i) Given any vector  $\underline{a} \in V_n$ , then the number of vectors  $\underline{x}$  such that  $\Delta(\underline{a}, \underline{x}) = k$  is  $\binom{n}{k}$ .
  - (ii) Given any vector  $\underline{a} \in V_n$  such that  $w(\underline{a}) = k$ , then the number of vectors  $\underline{b}$  of weight  $\ell$  such that  $\Delta(\underline{a}, \underline{b}) = i$  is given by

$$\begin{cases} 0 & \text{if } k + \ell - i \text{ is odd} \\ \binom{k}{\frac{1}{2}(k + \ell - i)} \binom{n - k}{\frac{1}{2}(\ell - k + i)} & \text{if } k + \ell - i \\ & \text{is even.} \end{cases}$$

Proof. (i) Given any vector  $\underline{a} \in V_n$ , we can find a translation such that  $\underline{a}$  is translated to the origin vector  $\underline{0}$ , the vector of all zeros. Applying this translation to all the vectors in  $V_n$  will not change distances between vectors, by Proposition 3.2. Then the vectors at distance  $k$  from our translated vector  $\underline{a}$  will simply be those vectors of weight  $k$ . The number of vectors of weight  $k$  is simply the number of ways to put  $k$  ones in the  $n$  coordinates, or  $\binom{n}{k}$ .

(ii) Let  $\underline{a}$  and  $\underline{b}$  be vectors of  $V_n$  such that  $w(\underline{a}) = k$  and  $w(\underline{b}) = \ell$ . Let  $x$  be the number of coordinates that they have in common. Then if  $\Delta(\underline{a}, \underline{b}) = i$ , we have  $i = (k - x) + (\ell - x) = k + \ell - 2x$  which implies  $2x = k + \ell - i$  or simply  $x = \frac{1}{2}(k + \ell - i)$ . Since  $x$  is an integer, then  $k + \ell - i$  must be even or else there are no vectors at distance  $i$ . If  $k + \ell - i$  is even, then we can choose  $x$  from the  $k$  coordinates and  $\ell - x$  from the remaining  $n - k$  coordinates, or simply  $\binom{k}{x} \binom{n - k}{\ell - x}$ , which gives  $\binom{k}{\frac{1}{2}(k + \ell - i)} \binom{n - k}{\frac{1}{2}(\ell - k + i)}$ .

QED





A vector  $\underline{a}$  of  $V_n$  may be identified with the subset  $B_{\underline{a}}$  of indices  $i$  of  $\{1, 2, \dots, n\}$  for which the  $i^{\text{th}}$  coordinate  $a_i$  of  $\underline{a}$  is one. For example, if  $\underline{a} = (0101)$ , then  $B_{\underline{a}} = \{2, 4\}$ . The set of indices in which the vectors  $\underline{a}$  and  $\underline{b}$  differ is the symmetric difference  $B_{\underline{a}} + B_{\underline{b}} = (B_{\underline{a}} \cup B_{\underline{b}}) \setminus (B_{\underline{a}} \cap B_{\underline{b}})$ . Thus  $\Delta(\underline{a}, \underline{b}) = |B_{\underline{a}} + B_{\underline{b}}|$ , where  $B_{\underline{a}} + B_{\underline{b}}$  is the symmetric difference of  $B_{\underline{a}}$  and  $B_{\underline{b}}$ ; i.e. the set of elements which are in one set but not both. For example, consider  $\underline{a} = (01110110)$  and  $\underline{b} = (10110101)$ . Then  $B_{\underline{a}} = \{2, 3, 4, 6, 7\}$  and  $B_{\underline{b}} = \{1, 3, 4, 6, 8\}$ . Then  $\Delta(\underline{a}, \underline{b}) = |B_{\underline{a}} + B_{\underline{b}}| = |\{1, 2, 7, 8\}| = 4$ . Clearly we have

Proposition 3.8. The existence of an  $(n, d; A)$ -code is equivalent to the existence of a class  $\beta$  of  $A$  subsets of an  $n$ -set  $X$  such that  $|B + B'| \geq d$  for distinct  $B, B'$  of  $\beta$ .

Further remarks on these ideas will be saved for Section 7.

## II. THE FUNCTION $A(n,d)$

### 4. Some Elementary Observations on the Function $A(n,d)$

We first note that the maximum number of codewords of a given code  $C$  may be viewed as a function  $A(n,d)$  depending on the length  $n$  and minimum distance  $d$  between its codewords. This section is concerned with some properties of the function  $A(n,d)$ .

Theorem 4.1. (Hamming [9]) If  $d$  is even,  $A(n,d) = A(n-1,d-1)$ .

Proof. Denote by  $|C|$  the number of codewords in the code  $C$ . Let  $C$  be an  $(n,d)$ -code such that  $|C| = A(n,d)$ . Define  $C'$  by  $C' = \{(a_1, a_2, \dots, a_{n-1}) : (a_1, a_2, \dots, a_{n-1}, a_n) \in C\}$ ; i.e. by dropping the last coordinate from each vector in  $C$ . Clearly  $C'$  is an  $(n-1, d-1)$ -code and since  $|C'| = |C|$  and  $|C| = A(n,d)$ , then  $A(n,d) \leq A(n-1, d-1)$ .

Next choose  $C'$  to be an  $(n-1, d-1)$ -code such that  $|C'| = A(n-1, d-1)$ . Define  $C''$  by  $C'' = \{(a_1, a_2, \dots, a_{n-1}, a_1 + \dots + a_{n-1}) : (a_1, a_2, \dots, a_{n-1}) \in C'\}$ ; i.e. by adding a parity check digit to each vector of  $C'$ , giving a code  $C''$  with codewords of only even weight. Clearly  $C''$  has length  $n$ . We want to show that the minimum distance between codewords in  $C''$  is  $d$ . Since  $d$  is even, then  $d-1$  is odd, so that the only way that two codewords of  $C'$  could be at distance  $d-1$  is if they were of different parity. But then the addition of the parity check digit must increase their distance to  $d$ . Thus  $C''$  is an  $(n,d)$ -code. Therefore, since  $|C''| = |C'|$  and  $|C'| = A(n-1, d-1)$ , we must have  $A(n-1, d-1) \leq A(n,d)$ .

Finally  $A(n,d) \leq A(n-1, d-1)$  and  $A(n-1, d-1) \leq A(n,d)$  imply  $A(n,d) = A(n-1, d-1)$ . QED

The above proposition demonstrates that to determine values for  $A(n,d)$ , we need only consider cases where  $d$  is odd, since  $d$  being even implies that consideration of an  $(n,d)$ -code could be reduced to the consideration of an  $(n-1,d-1)$ -code. For this reason, the table at the end of this paper will only list results for odd values of  $d$ .

The construction used in the proof of Theorem 4.1 can be modified to construct codes with words of only odd weight. We note this as

Theorem 4.2. If  $d$  is odd, then  $A(n,d) = A(n+1,d+1)$ . Furthermore, if there exists an  $(n,d;A)$ -code  $C$ , then there exist  $(n+1,d+1;A)$ -codes  $C'$  and  $C''$  such that the codewords of  $C'$  all are of even weight and those of  $C''$  all are of odd weight.

Proof. Given that  $d$  is odd,  $A(n,d) = A(n+1,d+1)$  follows directly from Theorem 4.1.

Next, if  $d$  is odd, then the only way for codewords of the  $(n,d)$ -code to be at distance  $d$  is if they have different parity. Consider  $C' = \{(a_1, a_2, \dots, a_n, a_1 + a_2 + \dots + a_n) : (a_1, a_2, \dots, a_n) \in C\}$  and  $C'' = \{(a_1, a_2, \dots, a_n, 1 + a_1 + \dots + a_n) : (a_1, a_2, \dots, a_n) \in C\}$ . These are both codes of length  $n+1$ . In each case, adding the parity check digit does not change the distance between codes of the same parity, but increases by one (to  $d+1$ ) the distance between codewords of different parity. Thus  $C'$  and  $C''$  are both  $(n+1,d+1)$ -codes. QED

The following result due to Plotkin [19] is very useful in deriving one bound for  $A(n,d)$  from another and provides many of the results for the table in Section 16.

Proposition 4.3.  $A(n-1,d) \leq A(n,d) \leq 2A(n-1,d)$ .

Proof. First we show  $A(n-1,d) \leq A(n,d)$ . Let  $C$  be an  $(n-1,d)$ -code such that  $|C| = A(n-1,d)$ . Define  $C' = \{(a_1, a_2, \dots, a_{n-1}, 0) : (a_1, a_2, \dots, a_{n-1}) \in C\}$ . Clearly  $C'$  has length  $n$  and the minimum distance between codewords is still at least  $d$ . Thus  $C'$  is an  $(n,d)$ -code and  $|C'| = A(n-1,d) \leq A(n,d)$ .

Next we show that  $A(n,d) \leq 2A(n-1,d)$ . Define  $C$  to be an  $(n,d)$ -code such that  $|C| = A(n,d)$ . Consider the partition of  $C$  into  $C_0 = \{(a_1, a_2, \dots, a_{n-1}) : (a_1, a_2, \dots, a_{n-1}, 0) \in C\}$  and  $C_1 = \{(a_1, a_2, \dots, a_{n-1}) : (a_1, a_2, \dots, a_{n-1}, 1) \in C\}$ ; i.e.  $C_0$  is formed from those codewords of  $C$  ending in zero and  $C_1$  from those ending in one. Clearly  $C_0$  and  $C_1$  are both of length  $n-1$  and the minimum distance between codewords in each is at least  $d$ ; i.e. both are  $(n-1,d)$ -codes. Then  $A(n,d) = |C| = |C_0| + |C_1| \leq A(n-1,d) + A(n-1,d) = 2A(n-1,d)$ . QED

Remark. It is easy to see that  $A(4,3) = 2$ . It follows from Proposition 4.3 that  $A(5,3) \leq 4$ ,  $A(6,3) \leq 8$  and  $A(7,3) \leq 16$ . This remark, together with examples 2.4 and 2.5, proves that  $A(6,3) = 8$  and  $A(5,3) = 4$ . We note that while such an exact determination is desirable, we must quite often settle for reasonably proximate upper and lower bounds for  $A(n,d)$  as no method is known to precisely determine its value in all cases.

Theorem 4.4. (Plotkin [19])  $A(2n,2d) \geq A(n,2d) A(n,d)$ .

Proof. Given  $\underline{a}, \underline{b}$  of  $V_n$ , we denote by  $(\underline{a}, \underline{b})$  the vector of length  $2n$  constructed by appending  $\underline{b}$  onto  $\underline{a}$ . For example, if  $\underline{a} = (a_1, a_2, \dots, a_n)$  and  $\underline{b} = (b_1, b_2, \dots, b_n)$ , then  $(\underline{a}, \underline{b}) =$



$(a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_n)$ . This construction is called concatenation. Let  $C_1$  be an  $(n, d)$ -code such that  $|C_1| = A(n, d)$  and  $C_2$  be an  $(n, 2d)$ -code such that  $|C_2| = A(n, 2d)$ . We will use concatenation to construct an  $(2n, 2d)$ -code  $C$  with  $A(n, d) A(n, 2d)$  codewords.

Define  $C = \{(\underline{a} + \underline{b}, \underline{a}) : \underline{a} \in C_1 \text{ and } \underline{b} \in C_2\}$ . The codewords of  $C$  will clearly be of length  $2n$  and it has  $A(n, d) A(n, 2d)$  distinct codewords since distinct pairs  $\underline{a}, \underline{b}$  will give distinct elements of  $C$ . We must show  $\Delta(\underline{c}_1, \underline{c}_2) \geq 2d$  for distinct  $\underline{c}_1, \underline{c}_2$  of  $C$ . Consider pairs  $\underline{a}_1, \underline{b}_1$  and  $\underline{a}_2, \underline{b}_2$  such that  $\underline{c}_1 = (\underline{a}_1 + \underline{b}_1, \underline{a}_1)$  and  $\underline{c}_2 = (\underline{a}_2 + \underline{b}_2, \underline{a}_2)$  are distinct. Then  $\underline{c}_1 + \underline{c}_2 = (\underline{a}_1 + \underline{b}_1, \underline{a}_1) + (\underline{a}_2 + \underline{b}_2, \underline{a}_2) = (\underline{a}_1 + \underline{b}_1 + \underline{a}_2 + \underline{b}_2, \underline{a}_1 + \underline{a}_2)$ . By Proposition 2.1,  $\Delta(\underline{c}_1, \underline{c}_2) = w(\underline{c}_1 + \underline{c}_2)$ . For distinct pairs  $\underline{a}_1, \underline{b}_1$  and  $\underline{a}_2, \underline{b}_2$  there are three possible cases:

Case 1. Suppose  $\underline{a}_1 = \underline{a}_2, \underline{b}_1 \neq \underline{b}_2$ . Then  $\underline{c}_1 + \underline{c}_2 = (\underline{a}_1 + \underline{b}_1 + \underline{a}_1 + \underline{b}_2, \underline{a}_1 + \underline{a}_1) = (\underline{b}_1 + \underline{b}_2, 0)$ . Therefore  $\Delta(\underline{c}_1, \underline{c}_2) = w(\underline{c}_1 + \underline{c}_2) = w(\underline{b}_1 + \underline{b}_2) \geq 2d$  since  $\underline{b}_1, \underline{b}_2$  are elements of  $C_2$ .

Case 2. Suppose  $\underline{a}_1 \neq \underline{a}_2, \underline{b}_1 = \underline{b}_2$ . Then  $\underline{c}_1 + \underline{c}_2 = (\underline{a}_1 + \underline{b}_1 + \underline{a}_2 + \underline{b}_1, \underline{a}_1 + \underline{a}_2) = (\underline{a}_1 + \underline{a}_2, \underline{a}_1 + \underline{a}_2)$ . Then  $\Delta(\underline{c}_1, \underline{c}_2) = w(\underline{c}_1 + \underline{c}_2) = w(\underline{a}_1 + \underline{a}_2) + w(\underline{a}_1 + \underline{a}_2) \geq d + d = 2d$  since  $\underline{a}_1, \underline{a}_2$  are elements of  $C_1$ .

Case 3. Suppose  $\underline{a}_1 \neq \underline{a}_2, \underline{b}_1 \neq \underline{b}_2$ . Then  $\Delta(\underline{c}_1, \underline{c}_2) = w(\underline{c}_1 + \underline{c}_2) = w(\underline{a}_1 + \underline{b}_1 + \underline{a}_2 + \underline{b}_2) + w(\underline{a}_1 + \underline{a}_2) \geq w(\underline{b}_1 + \underline{b}_2) \geq 2d$  since  $\underline{b}_1, \underline{b}_2$  are elements of  $C_2$ .

The result follows easily. QED

5. Some Bounds on  $A(n,d)$ 

Let  $\underline{a}$  be a vector in  $V_n$ . By the sphere  $S_d(\underline{a})$  of radius  $d$  about  $\underline{a}$  we mean the set of vectors which are at most distance  $d$  from  $\underline{a}$ ; i.e.

$$S_d(\underline{a}) = \{\underline{b} : \underline{b} \in V_n, \Delta(\underline{a}, \underline{b}) \leq d\}.$$

Proposition 5.1. (Gilbert-Varsharmov Bound [4] [32])

$$A(n,d) \geq \frac{2^n}{\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{d-1}}.$$

Proof. If  $C$  is an  $(n,d)$ -code such that  $|C| = A(n,d)$ , consider the spheres of radius  $d-1$  around each codeword. Clearly they must exhaust all vectors of  $V_n$ . To see how many vectors are contained in each sphere, we must find how many are at most distance  $d-1$  from it. From Proposition 3.7 (i), this is  $\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{d-1}$ . Since there are  $A(n,d)$  distinct codewords there are  $A(n,d)[\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{d-1}]$  vectors in all the spheres. Since each of the  $2^n$  vectors of  $V_n$  is in at least one of these spheres, the result follows immediately. QED

Rao [28] also considered the sphere packing problem, later investigated by Hamming as presented in

Theorem 5.2. (Hamming's Sphere Packing Bound [9]) If  $d = 2e + 1$ , then  $A(n,d) \leq \frac{2^n}{\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{e}}$ .

Proof. Consider the spheres of radius  $e$  about the codewords of an  $(n,d)$ -code  $C$  where  $|C| = A(n,d)$ . If  $\underline{a}$  and  $\underline{b}$  are distinct codewords of  $C$ , then  $S_e(\underline{a}) \cap S_e(\underline{b}) = \emptyset$  using the triangle inequality and  $\Delta(\underline{a}, \underline{b}) \geq 2e + 1$ . Then since each sphere contains  $\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{e}$  vectors and since the total number of vectors in  $V_n$  is  $2^n$ , we have  $2^n \geq |C| [\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{e}]$  and the result follows. QED

An  $(n, 2e + 1)$ -code is defined to be perfect (or close packed) if strict equality holds in the sphere packing bound; i.e. if

$$|C| = \frac{2^n}{\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{e}}.$$

Geometrically, this happens when there are no vectors lying outside the spheres of radius  $e$  about the codewords. Note that for  $C$  to be a perfect code,  $\frac{2^n}{\binom{n}{0} + \dots + \binom{n}{e}}$  must be an integer and  $\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{e}$

must be a power of 2. As will be presented in Proposition 6.4, Hamming has shown that for  $e = 1$  this occurs when  $n = 2^m - 1$  where  $m$  is any positive integer. In the case  $e = 2$ , Joshi [12] notes that  $\binom{n}{0} + \binom{n}{1} + \binom{n}{2}$  is a power of 2 only for  $n = 2, 5$ , and 90 where  $\binom{90}{0} + \binom{90}{1} + \binom{90}{2} = 2^{12}$ . Joshi further proves that the only perfect  $(n, 7)$ -codes are the cyclic Golay  $(23, 7)$ -code (mentioned in Section 8) and the trivial  $(7, 7)$ -code. In fact, the only nontrivial perfect binary codes are the Hamming codes and the Golay  $(23, 7)$ -code [23]. As a point of interest, we note that  $\binom{23}{0} + \binom{23}{1} + \binom{23}{2} + \binom{23}{3} = 2^{11}$ . Further observations on the symmetries of close packed codes and the existence problem for  $e \geq 2$  are presented by Shapiro and Slotnick [22].

Theorem 5.3. (Plotkin's Bound [19]). If  $2d > n$ , then  $A(n, d) \leq 2t \leq \frac{2d}{2d - n}$ ,  $t$  an integer. In other words,  $A(n, d)$  is less than or equal to the largest even integer in  $\frac{2d}{2d - n}$ .

Proof. Let  $C$  be an  $(n, d; A)$ -code. Then by Proposition 3.8, we can find a class  $\beta$  of  $A$  subsets of an  $n$ -set  $X$  such that  $|B_1 \cap B_2| \geq d$  for distinct  $B_1, B_2$  of  $\beta$ .

Let  $X_i$  denote the set of elements  $x$  of  $X$  which are contained in exactly  $i$  of the sets  $B_j$  of  $\beta$ .

$$\text{Define } I(x, B_j) = \begin{cases} 1 & \text{if } x \in B_j \\ 0 & \text{if } x \notin B_j \end{cases}$$

Consider  $\sum_{\{B_1, B_2\}} |B_1 + B_2|$  where the sum is extended over all  $\binom{A}{2}$

unordered pairs  $\{B_1, B_2\}$  of distinct subsets  $B_1, B_2$  of  $\beta$ . Then

$$\begin{aligned} \binom{A}{2} d &\leq \sum_{\{B_1, B_2\}} |B_1 + B_2| = \sum_{\{B_1, B_2\}} \sum_{x \in X} I(x, B_1 + B_2) \\ &= \sum_{i=0}^A \sum_{x \in X_i} \left( \sum_{\{B_1, B_2\}} I(x, B_1 + B_2) \right) = \sum_{i=0}^A \sum_{x \in X_i} (A - i) i \\ &= \sum_{i=0}^A i(A - i) |X_i| \leq n \max_{0 \leq i \leq A} i(A - i). \end{aligned}$$

In short,  $\binom{A}{2} d \leq n \max_{0 \leq i \leq A} i(A - i)$ . Since  $A$  is either even or odd,

then  $A = 2t$  or  $A = 2t - 1$  for some integer  $t$ . Then

$$\binom{2t-1}{2} d \leq nt(t-1) \text{ or } \binom{2t}{2} d \leq nt^2 \text{ so that } (2t-1)(t-1)d \leq nt(t-1)$$

$$\text{or } t(2t-1)d \leq nt^2. \text{ Thus } \frac{n}{d} \geq \frac{2t-1}{t} = 2 - \frac{1}{t} \text{ so that } \frac{n-2d}{d} \geq -\frac{1}{t}$$

$$t \leq \frac{d}{2d-n} \text{ and finally } A \leq 2t \leq \frac{2d}{2d-n}. \text{ QED}$$

By applying a result from Section 4, the following corollary provides an improvement to Plotkin's bound, often giving the best known upper bound for  $A(n, d)$ .

Corollary 5.4. If  $d$  is odd and  $2d \geq n$ , then  $A(n, d) \leq \frac{2d+2}{2d-n+1}$ .

Proof. If  $d$  is odd, then by Theorem 4.2 we have  $A(n, d) =$

$A(n+1, d+1)$ . By Theorem 5.3,



$$A(n,d) = A(n+1,d+1) \leq \frac{2(d+1)}{2(d+1) - (n+1)} = \frac{2d+2}{2d-n+1} \cdot \text{QED}$$

Corollary 5.5.  $A(n,n) = 2$ .

Proof. By Theorem 5.3,  $A(n,n) \leq 2$  and the vectors of all zeros and all ones provide an example showing  $A(n,n) \geq 2$ . QED

Corollary 5.6.  $A(4m-1, 2m) \leq 4m$  and  $A(4m-2, 2m) \leq 2m$ .

Proof. The proof follows directly from Theorem 5.3.

Corollary 5.7.  $A(4m, 2m) \leq 8m$ .

Proof. By Proposition 4.3,  $A(4m, 2m) \leq 2A(4m-1, 2m)$ . Then by Corollary 5.6,  $2A(4m-1, 2m) \leq 8m$ , giving  $A(4m, 2m) \leq 8m$ . QED

In [19], Plotkin proved that given a prime of the form  $4m-1$ , then  $A(4m, 2m) = 8m$ . The existence of one of these optimal  $(4m, 2m; 8m)$ -codes is equivalent to the existence of a Hadamard matrix of order  $4m$ . Further discussion concerning the existence of Hadamard matrices and their use in code construction is presented in Section 10.

### III. CONSTRUCTION OF CODES

As we have already stated, a lower bound for  $A(n,d)$  is generally determined by the actual construction of a code of length  $n$  and minimum distance between codewords at least  $d$ . The following sections present the constructions most relevant to the development of the table in Section 16.

#### 6. Linear Codes and Hamming Codes

As was mentioned in Section 1,  $V_n$  may be considered as a vector space of dimension  $n$  over the field  $Z_2$ . We defined a linear code  $C$  as a subset of  $V_n$  which is also a subspace. While linear codes do not always give the greatest number of codewords for a given length  $n$  and minimum distance  $d$ , they are important in that they are practically implementable through their matrix representation.

Let  $C$  be a linear code with block length  $n$ . The set of codewords of  $C$  can be considered as a vector subspace of  $V_n$ . Suppose that  $C$  is of dimension  $k$ . Any set of  $k$  basis vectors for  $C$  can be considered as rows of an  $k \times n$  matrix  $G$ , say

$$G = \begin{bmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & & \vdots \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{bmatrix}.$$

Then a vector of length  $n$  is a codeword of  $C$  iff it is a linear combination of rows of  $G$ . If any two linear combinations were equal, there would be a dependence relation among rows of  $G$ ; therefore, each distinct linear combination gives a distinct codeword. Since there are

$k$  coefficients in our linear combination of  $k$  basis vectors and two choices for each coefficient, there are  $2^k$  codewords in  $C$ .

The messages for  $C$  are the  $2^k$  binary  $k$ -tuples. If  $\underline{a} = (a_1, a_2, \dots, a_k)$  is any binary  $k$ -tuple, then  $\underline{a}G$  is a codeword. The matrix  $G$  is called the generating matrix for  $C$ . Unless  $k$  is relatively small, the matrix description is much more compact than a list of the  $2^k$  codewords.

Remark. Since the set of basis vectors for a subspace is not unique, the generating matrix is also not unique.

Example 6.1. Consider a linear code  $C$  of block length 7 with generating matrix

$$G = \begin{bmatrix} 1000111 \\ 0100011 \\ 0010101 \\ 0001110 \end{bmatrix}.$$

The messages are the sixteen possible binary 4-tuples. If we consider the message  $(0011)$ , then its corresponding codeword is  $(0011)G = (0011011)$ . The remaining fifteen codewords are found in a similar manner.

There is an alternate description of  $C$  through matrices. We first consider several definitions. For  $\underline{x}, \underline{y}$  of  $V_n$  where  $\underline{x} = (x_1, x_2, \dots, x_n)$  and  $\underline{y} = (y_1, y_2, \dots, y_n)$ , let  $\underline{x} \cdot \underline{y}$  denote the standard inner product

$$(x_1, x_2, \dots, x_n) \cdot (y_1, y_2, \dots, y_n) = x_1 y_1 + x_2 y_2 + \dots + x_n y_n.$$

Next, suppose  $C$  is a  $k$ -dimensional subspace of  $V_n$ . Then the orthogonal space of  $C$ , denoted  $C^\perp$  and defined by  $C^\perp = \{\underline{x} : \underline{x} \cdot \underline{c} = 0 \text{ for every } \underline{c} \text{ in } C\}$ , is a subspace of  $V_n$  of dimension  $n - k$  (see [18, p.36]). Consider

this orthogonal space of  $C$ . Any set of  $n - k$  basis vectors for  $C^\perp$  can be considered as the columns of an  $n \times (n - k)$  matrix  $H$ , say

$$H = \begin{bmatrix} h_{11} & h_{12} & \cdots & h_{1,n-k} \\ h_{21} & h_{22} & \cdots & h_{2,n-k} \\ \vdots & \vdots & & \vdots \\ h_{n1} & h_{n2} & \cdots & h_{n,n-k} \end{bmatrix}.$$

The matrix  $H$  is called a parity check matrix for  $C$ . By construction, a binary  $n$ -tuple is a codeword of  $C$  iff it is orthogonal to every column of  $H$ ; i.e.  $\underline{c}$  is in  $C$  iff  $\underline{c}H = \underline{0}$ . The code  $C$  is said to be the null space of the matrix  $H$ .

Example 6.2. Consider the code  $C$  of block length 7 presented in example 6.1. The orthogonal space  $C^\perp$  of  $C$  is of dimension 3 and has as a basis the vectors (1011100), (1101010) and (1110001). These vectors can be used as columns to construct a  $7 \times 3$  parity check matrix  $H$  for  $C$  where

$$H = \begin{bmatrix} 111 \\ 011 \\ 101 \\ 110 \\ 100 \\ 010 \\ 001 \end{bmatrix}.$$

Since  $(0011011)H = (000)$ , it follows that (0011011) is a codeword of  $C$ .

Thus far we have mentioned nothing about the minimum distance of our linear code  $C$ . This is determined as in

Theorem 6.3. Let  $n = k + r$ . The following conditions are equivalent:

- (i) The existence of a  $k$ -dimensional linear code  $C$  of length  $n$



with  $\Delta(\underline{a}, \underline{b}) \geq d$  for distinct codewords  $\underline{a}, \underline{b}$  of  $C$ ;

(ii) The existence of a set  $\{\underline{u}_1, \underline{u}_2, \dots, \underline{u}_n\}$  of  $n$   $r$ -tuples such that no  $d-1$  of the  $\underline{u}_i$  are linearly dependent.

Proof. Given a  $k$ -dimensional linear code  $C$  of length  $n$ , let  $\underline{x}_1, \underline{x}_2, \dots, \underline{x}_r$  be a basis for its  $r$ -dimensional orthogonal space  $C^\perp$ . Form the  $n \times r$  matrix  $H$  whose columns are  $\underline{x}_1, \underline{x}_2, \dots, \underline{x}_r$  and let  $\underline{u}_1, \underline{u}_2, \dots, \underline{u}_n$  denote the row vectors of  $H$ .

$$H = \begin{array}{cccc} \underline{x}_1 & \underline{x}_2 & \dots & \underline{x}_r \\ \begin{bmatrix} a_{11} & a_{21} & \dots & a_{r1} \\ a_{12} & a_{22} & \dots & a_{r2} \\ \vdots & \vdots & & \vdots \\ a_{1n} & a_{2n} & \dots & a_{rn} \end{bmatrix} & \begin{matrix} \underline{u}_1 \\ \underline{u}_2 \\ \vdots \\ \underline{u}_n \end{matrix} \end{array}$$

We note that if

$\underline{x}_1 = (a_{11}, a_{12}, \dots, a_{1n})$ ,  $\underline{x}_2 = (a_{21}, a_{22}, \dots, a_{2n})$ , ...,  $\underline{x}_r = (a_{r1}, a_{r2}, \dots, a_{rn})$ , then  $\underline{u}_1 = (a_{11}, a_{21}, \dots, a_{r1})$ , ...,  $\underline{u}_n = (a_{1n}, a_{2n}, \dots, a_{rn})$ .

Then for  $\underline{c} = (c_1, c_2, \dots, c_n)$  of  $V_n$ , we have

$$\begin{aligned} & (\underline{c}\underline{x}_1, \underline{c}\underline{x}_2, \dots, \underline{c}\underline{x}_r) \\ &= (c_1 a_{11} + c_2 a_{12} + \dots + c_n a_{1n}, c_1 a_{21} + c_2 a_{22} + \dots + c_n a_{2n}, \dots, \\ & \quad c_1 a_{r1} + c_2 a_{r2} + \dots + c_n a_{rn}) \\ &= (c_1 a_{11}, c_1 a_{21}, \dots, c_1 a_{r1}) + \dots + (c_n a_{1n}, \dots, c_n a_{rn}) \\ &= c_1 (a_{11}, a_{21}, \dots, a_{r1}) + \dots + c_n (a_{1n}, a_{2n}, \dots, a_{rn}) \\ &= c_1 \underline{u}_1 + c_2 \underline{u}_2 + \dots + c_n \underline{u}_n. \end{aligned}$$

Thus  $\underline{c}$  is in  $C$  iff  $c_1 \underline{u}_1 + c_2 \underline{u}_2 + \dots + c_n \underline{u}_n = \underline{0}$ . If no  $d-1$  of  $\underline{u}_1, \underline{u}_2, \dots, \underline{u}_n$  are dependent, then  $C$  cannot contain a nonzero vector of weight less than  $d$ . If it did, say if there were a  $\underline{c}$  in  $C$  such that

$w(\underline{c}) = d - 1$ , where  $\underline{c} = (c_1, c_2, \dots, c_n)$ , then  $\underline{c}$  has  $d - 1$  nonzero coordinates and we have

$$c_1 \underline{u}_1 + c_2 \underline{u}_2 + \dots + c_{d-1} \underline{u}_{d-1} + 0 \underline{u}_d + 0 \underline{u}_{d+1} + \dots + 0 \underline{u}_n = \underline{0},$$

contradicting that no  $d - 1$  are dependent. Since  $d$  is the minimum weight of codewords of  $C$  and  $C$  is linear, then Proposition 2.3 provides that the minimum distance between distinct nonzero codewords is at least  $d$ . And conversely. QED

We noted in Section 3 that two codes are equivalent if one can be obtained from the other by means of a combination of translations and permutations. In terms of the matrix representation of linear codes, two codes are equivalent if their generating matrices are combinatorially equivalent; i.e. if one matrix can be obtained from the other by means of row operations and column permutations. In particular, each generating matrix is equivalent to a matrix in echelon canonical form, which provides a code having information symbols in the first  $k$  positions and check symbols in the remaining  $n - k$  positions. Peterson [18,p.46] has taken this to be the definition of a  $k$ -dimensional systematic code, in which case it can be said that every linear code is equivalent to a systematic code. We use the term systematic in a more general sense. As noted in Section 2, we define a systematic  $k$ -dimensional code to be a code with information symbols in any  $k$  coordinates. For example, the code defined by the vectors (0001), (0011), (1101), and (1111) has the second and third coordinates as information positions. By our definition, every linear code is systematic, but the converse need not be true.

In order to consider the error correcting capabilities of a linear code, we first define the syndrome of a vector. Let  $C$  be a linear code with parity check matrix  $H$ . If  $\underline{x}$  is any vector of  $V_n$ , then the syndrome of  $\underline{x}$  is defined by  $\underline{s} = \underline{x}H$ , where  $\underline{s}$  is a row vector of length equal to the dimension of  $C^\perp$ . Recalling that  $\underline{c}$  is a codeword of  $C$  iff  $\underline{c}H = \underline{0}$ , then the codewords are precisely those vectors with syndrome zero.

For example, if  $\underline{x}$  is a binary 15-tuple and  $H$  is a  $15 \times 4$  matrix, then  $\underline{x}H$  is a vector of length 4. If  $\underline{u}_1, \underline{u}_2, \dots, \underline{u}_{15}$  are the row vectors of  $H$  and  $\underline{x} = (x_1, x_2, \dots, x_{15})$ , then the syndrome of  $\underline{x}$  is  $x_1\underline{u}_1 + x_2\underline{u}_2 + \dots + x_{15}\underline{u}_{15}$ .

Let  $C$  be a code with minimum distance between codewords at least 3. If a codeword  $\underline{c}$  is transmitted across a noisy channel and one error occurs, then a vector  $\underline{b}$  is received with  $\Delta(\underline{c}, \underline{b}) = 1$ . Since the minimum distance between distinct codewords is at least 3, we could determine the transmitted codeword by examining the list of codewords until one adjacent to  $\underline{b}$  was found. If the list is small, this is not difficult, but by using syndromes the problem becomes much easier no matter how large the list of codewords may be. If  $\underline{c}$  is the transmitted codeword and  $\underline{b}$  the received word, then  $\underline{b} = \underline{c} + \underline{e}$  where  $\underline{e}$  is called the error vector, is of the same length as  $\underline{b}$  and  $\underline{c}$  and has a one in every coordinate in which they differ; i.e. in which an error has occurred. Since  $\underline{b}H = (\underline{c} + \underline{e})H = \underline{c}H + \underline{e}H = \underline{0} + \underline{e}H = \underline{e}H$ , the syndrome of the received word is the same as the syndrome of the error vector. If  $\underline{b}H = \underline{0}$ , then  $\underline{b}$  is a codeword and we must assume that no errors occurred in transmission (although this may not be the case). If  $\underline{b}H$  is not equal to  $\underline{0}$  ( $\underline{b}$  is not a codeword) and we assume that only one error

occurred in transmission, then the error vector  $\underline{e}$  has a single one, say in the  $i^{\text{th}}$  coordinate, and the syndrome of  $\underline{b}$  equals the syndrome of  $\underline{e}$  equals  $\underline{u}_i$ , the  $i^{\text{th}}$  row of  $H$ . Thus if a single error has occurred, then the syndrome of the received word matches one of the rows of  $H$ , giving the coordinate in which the error has occurred. This will become clearer from the example following the next proposition.

The following result due to Hamming [9] guarantees the existence of perfect codes for specific  $n$ . The codes thus determined are called Hamming codes.

Proposition 6.4. If  $n = 2^r - 1$  for some positive integer  $r$ , then  $A(n, 3) = 2^{n-r}$ .

Proof. By Theorem 5.2,  $A(n, 3) \leq \frac{2n}{1+n} = \frac{2n}{1+2^r-1} = 2^{n-r}$ . Next form a matrix whose rows are all nonzero  $r$ -tuples. Since no two rows are linearly dependent, Theorem 6.3 guarantees the existence of an  $(n-r)$ -dimensional linear code  $C$  with minimum distance between codewords at least 3. QED

Remark. For  $n = 2^r - 2$ , we also have that  $A(n, 3) = 2^{n-r}$ . This result follows directly from Proposition 6.5 and Proposition 13.5.

As an example, consider the case when  $r = 4$  so that  $n = 15$ . By Proposition 6.4, there is a code  $C$  which is an  $(15, 3; 2^{11})$ -code; i.e.  $C$  has 11 information digits. To determine  $C$ , first form a matrix  $H$  whose rows are all possible nonzero vectors of  $\{GF(2)\}^4$ .



$$H = \begin{bmatrix} 1111 \\ 1110 \\ 0111 \\ 1101 \\ 1011 \\ 1100 \\ 0110 \\ 0011 \\ 1001 \\ 1010 \\ 0101 \\ 1000 \\ 0100 \\ 0010 \\ 0001 \end{bmatrix}$$

Consider the 11-dimensional linear code  $C$  whose codewords are those vectors  $\underline{c} = (c_1, c_2, \dots, c_{15})$  satisfying the matrix equation  $\underline{c}H = \underline{0} = (0000)$ . Equivalently,

$$c_1 + c_2 + c_4 + c_5 + c_6 + c_9 + c_{10} + c_{12} = 0$$

$$c_1 + c_2 + c_3 + c_4 + c_6 + c_7 + c_{11} + c_{13} = 0$$

$$c_1 + c_2 + c_3 + c_5 + c_7 + c_8 + c_{10} + c_{14} = 0$$

$$c_1 + c_3 + c_4 + c_5 + c_8 + c_9 + c_{11} + c_{15} = 0$$

where these equations are obtained by completing the multiplication of  $\underline{c}H$ . These equations are called the parity check equations and  $H$  is the parity check matrix. Since every codeword is orthogonal to the four column vectors of  $H$  and no two rows are linearly dependent, then  $C$  can contain no codewords of weight 1 or 2. Since  $C$  is linear, the preceding statement implies that the minimum distance between codewords is at least 3, and so  $C$  is an  $(15, 3; 2^{11})$ -code. Since the last four rows of  $H$  are independent, we may consider the first eleven positions as information symbols and thus the four remaining check symbols are determined by

$$c_{12} = c_1 + c_2 + c_4 + c_5 + c_6 + c_9 + c_{10}$$

$$c_{13} = c_1 + c_2 + c_3 + c_4 + c_6 + c_7 + c_{11}$$

$$c_{14} = c_1 + c_2 + c_3 + c_5 + c_7 + c_8 + c_{10}$$

$$c_{15} = c_1 + c_3 + c_4 + c_5 + c_8 + c_9 + c_{11}$$

from the parity check equations.

We will use the preceding example to demonstrate the use of syndromes to correct a single error in transmission. For example, if the received word is  $\underline{b} = (010101011001001)$ , the syndrome of  $\underline{b}$  is  $\underline{bH} = (1100)$ . Since the syndrome of  $\underline{b}$  is not  $\underline{0}$ ,  $\underline{b}$  is not a codeword. If we assume that only one error occurred and note that the syndrome of  $\underline{b}$  is equal to the sixth row of  $H$ , then the error will have occurred in the sixth coordinate and the transmitted codeword was actually  $(010100011001001)$ . Of course, since several errors might have occurred, this may be the wrong answer. We note that the possible error vectors form the coset  $C + \underline{b}$  of  $C$ .

Proposition 6.5. If  $n \leq 2^r - 1$ , then  $A(n,3) \geq 2^{n-r}$ .

Proof. For  $n \leq 2^r - 1$ , take as parity check matrix  $H$  an  $n \times r$  matrix whose rows are all distinct and nonzero. The result follows from Theorem 6.3. QED

Another important family of linear codes are those determined by circulant matrices. A circulant matrix is one in which each row is a cyclic shift of the previous row by one place. In [14] Karlin showed that the generator matrix  $G$  of many linear codes of length  $n$  and dimension  $k$  can be represented in echelon canonical form as a  $k \times k$  identity matrix  $I$  and one or more circulant matrices forming

the remaining  $k \times (n - k)$  section of  $G$  which determines the check digits. A code defined in this manner is called a circulant (or quasicyclic) code.

As an example, he noted that the generating matrix for the Golay  $(23,7;2^{12})$ -code can be written as

$$\left[ \begin{array}{c|cccccc} 1 & & & & & \\ & 1 & & & & \\ & & \ddots & & & \\ & & & \ddots & & \\ & & & & 1 & \\ & & & & & 1 \end{array} \right] \begin{array}{c} \\ \\ \\ C \\ 11 \dots 1 \end{array}$$

where  $C$  is a circulant matrix whose first row has a one in the first position and in the positions corresponding to the quadratic residues modulo 11; i.e. the first row is 11011100010. He further showed that many quadratic residue codes (discussed in Section 8) may be defined by such generating matrices.

## 7. Cyclic Codes and Codes Based on Groups

Define  $C$  to be a cyclic code of length  $n$  if a cyclic shift of any codeword in  $C$  is also a codeword; i.e. if

$\underline{a} = (a_{n-1}, a_{n-2}, \dots, a_1, a_0)$  is a codeword, then so is the vector  $\underline{a}' = (a_{n-2}, \dots, a_0, a_{n-1})$ . We note that polynomial codes are frequently defined as being equivalent to cyclic codes, but that for us polynomial codes are codes which are both cyclic and linear. Polynomial codes will be discussed in Section 8.

One class of nonlinear cyclic codes is derived from quadratic residues. Let  $n$  be a prime of the form  $n = 4m + 1$ . Define the vectors  $\underline{a}$  and  $\underline{b}$  by  $\underline{a} = (a_0, a_1, \dots, a_{n-1})$  where  $a_0 = 0$  and  $a_i = 1$  if  $i$  is a quadratic residue modulo  $n$  and  $a_i = 0$  otherwise, and  $\underline{b} = (b_0, b_1, \dots, b_{n-1})$  where  $b_0 = 0$  and  $b_i = 1 - a_i$  for  $1 \leq i \leq n - 1$ . Then define a code  $C$  to consist of all  $2n$  cyclic shifts of  $\underline{a}$  and  $\underline{b}$ , plus the vector of all zeros and the vector of all ones. We present the following proposition, whose proof may be found in Sloane and Whitehead [26]:

Proposition 7.3.  $C$  is a cyclic  $(4m + 1, 2m; 8m + 4)$ -code.

We note that for  $m = 4$  we get an  $(17, 8; 36)$ -code from which we can derive an  $(16, 7; 36)$ -code by deleting one coordinate. This latter code provides us with the best known result for these values of  $n$  and  $d$ .

Further results for primes of the form  $4m + 1$  are found in Joshi [12] and presented as

Proposition 7.4. If  $4m + 1$  is a prime, then



- (i) there exists an  $(4m, 2m; 4m + 2)$ -code,
- (ii) there exists an  $(4m, 2m - 2; 8m + 4)$ -code, and
- (iii) if  $4m + 1 > 5$ , there exists an  
 $(4m, 2m - [\sqrt{4m + 1}] - 1; 16m + 4)$ -code.

For primes of the form  $4m + 1$ , Plotkin [19] provides the following results:

Proposition 7.5. If  $4m + 1$  is a prime, then  $A(4m, 2m) = 8m$ .

Proof. See Plotkin.

Corollary 7.6. If  $A(4m, 2m) = 8m$ , then  $A(8m, 4m) = 16m$ .

Proof. By Theorem 4.4,  $A(8m, 4m) \geq A(4m, 4m) A(4m, 2m) = 2A(4m, 2m) = 16m$ . From Corollary 5.6, we get  $A(8m, 4m) \leq 16m$ . But then  $A(8m, 4m) = 16m$ . QED

There are other constructions for codes which involve groups. Before presenting several examples, we make some observations.

Let  $B$  be a subset of an abelian group  $G$  and consider the translates  $B + g$  where  $g$  is an element of  $G$ . In particular, consider an arbitrary subgroup  $B$  of the abelian group  $Z_n$  and look at  $B + 0, B + 1, \dots, B + (n-1)$ . We are interested in developing a code from such translates. Recalling Proposition 3.8, by determining  $(B + i) + (B + j)$  and then  $|(B + i) + (B + j)|$  we can evaluate the distances between prospective codewords. Using an alternate approach, we first consider

Proposition 7.7. If  $A$  and  $B$  are subsets of an abelian group  $G$ , then  $|(A + i) \cap (B + j)|$  is equal to the number of times  $(j - i)$  occurs in the list of differences  $(a - b : a \in A, b \in B)$ .

Proof. We must exhibit a 1 - 1 correspondence between the elements of  $(A + i) \cap (B + j)$  and the set of ordered pairs  $(a, b)$  with  $a \in A$ ,  $b \in B$  and  $a - b = j - i$ . If  $x \in (A + i) \cap (B + j)$ , then  $x = a + i$  and  $x = b + j$  for some  $a \in A$ ,  $b \in B$ . Thus  $a + i = b + j$  and  $a - b = j - i$ . It is easily checked that the mapping  $x \mapsto (x - i, x - j)$  and its inverse  $(a, b) \mapsto a + i (= b + j = x)$  provides such a correspondence. QED

As a direct result of the preceding proposition, we present the following corollary without proof:

Corollary 7.8. If  $B + i$  and  $B + j$  are two translates of the set  $B$ , then  $|(B + i) \cap (B + j)|$  is equal to the number of times that  $(j - i)$  occurs when considering the differences between elements of  $B$ .

Remark. If  $B$  has  $k$  elements, say  $B = \{b_1, b_2, \dots, b_k\}$ , then there are  $k(k - 1)$  nonzero differences  $b_i - b_j$  for  $i \neq j$ .

Remark. If  $A = B$ , then  $|A \cap (A + g)|$  is equal to the number of times  $g$  occurs in the list of differences  $a - b$  for  $a, b$  in  $A$ . This is a special case of Corollary 7.8 and is useful in determining the number of elements that a given set has in common with any of its translates.

For example, consider the abelian group  $Z_{11}$  and a subset  $D = \{1, 3, 4, 5, 9\}$ . The differences between the elements of  $D$  are  $\pm 2, \pm 3, \pm 4, \pm 3, \pm 1, \pm 2, \pm 5, \pm 1, \pm 5$ , and  $\pm 4$ . Then, for example, the number 3 occurs as a difference twice so that Corollary 7.8 guarantees that  $D$  and  $D + 3$  have two elements in common.

To demonstrate the usefulness of these remarks, consider the group  $Z_7$  and look at the subset  $S = \{0,1,3\}$ . We can represent  $S$  by a 7-tuple  $\underline{a} = (a_0, a_1, \dots, a_6)$  where  $a_i = 1$  iff  $i$  is in  $S$  and  $a_i = 0$  otherwise. Thus the vector representation for  $S$  is  $(1101000)$ . Consider another representation,  $(013)$ , where  $i$  is in this vector whenever  $a_i = 1$  in  $\underline{a}$ . The subsets obtained from the cyclic shifts of this vector by consecutive addition of  $(111)$  to  $(013)$  are  $\{0,1,3\}$ ,  $\{1,2,4\}$ ,  $\{2,3,5\}$ ,  $\{3,4,6\}$ ,  $\{4,5,0\}$ ,  $\{5,6,1\}$ , and  $\{6,0,2\}$ . From Proposition 7.7 and its corollaries, these seven translates of  $S$  have at most one element in common; therefore, the corresponding seven 7-tuples of weight three have minimum distance at least four between them. Next consider the complement of  $S$  in  $Z_7$ , namely  $T = \{2,4,5,6\}$ , which can be represented by the 7-tuple  $(0010111)$ . The subsets obtained from the cyclic shifts of the representation  $(2456)$  are  $\{2,4,5,6\}$ ,  $\{3,5,6,0\}$ ,  $\{4,6,0,1\}$ ,  $\{5,0,1,2\}$ ,  $\{6,1,2,3\}$ ,  $\{0,2,3,4\}$ , and  $\{1,3,4,5\}$ . Since the differences between distinct elements of  $T$  are  $\pm 2, \pm 3, \pm 3, \pm 1, \pm 2, \pm 1$ , then two subsets have at most two elements in common and the corresponding seven 7-tuples of weight four have minimum distance at least four between them. Next consider the list of differences  $D$  between elements of  $S$  and those of  $T$ ; i.e.  $D = \{a - b : a \in S, b \in T\}$ . Then  $D = \{2,4,5,6,1,3,4,5,-1,1,2,3\}$  and the translates of  $T$  have at most two elements in common with the translates of  $S$ . But then a vector of weight three representing a translate of  $S$  can have at most two coordinates in common with a vector of weight four representing a translate of  $T$ . But then the minimum distance between the seven vectors of weight three and those of weight four is at least three. By adding

the vector of all zeros and the vector of all ones, we get a cyclic  $(7,3;16)$ -code proving  $A(7,3) \geq 16$ . But Hamming's bound gives  $A(7,3) \leq 16$  so that  $A(7,3) = 16$ .

We now present a noncyclic code determined by the group  $G = Z_3 \times Z_3$ . This group has nine elements of the form  $(i,j)$  for  $i$  and  $j$  in  $Z_3$  and is representable by a  $3 \times 3$  matrix  $M$  whose entries are the nine possible pairs  $ij$  of elements of  $Z_3$ .

$$M = \begin{bmatrix} 00 & 01 & 02 \\ 10 & 11 & 12 \\ 20 & 21 & 22 \end{bmatrix}$$

Next consider the nine distinct subsets  $S_{ij}$  of  $G$  obtained by considering each of these nine elements  $ij$  and including in  $S_{ij}$  those elements remaining after removing the row and column containing  $ij$ ; i.e. the  $i^{\text{th}}$  row and the  $j^{\text{th}}$  column. For example, if  $ij$  is 00, then  $S_{00} = \{11, 12, 21, 22\}$ . The remaining eight  $S_{ij}$  can be found by taking the translates of  $S_{00}$  by elements  $g$  of  $G$ ,  $S_{00} + g$ , considering addition to be normal coordinatewise addition in  $G$  modulo 3. By assigning each of the nine elements of  $G$  to a coordinate position of a 9-tuple, we can derive a vector representation for the subsets  $S_{ij}$ . If the assignment were by the correspondence

$$(1,2,3,4,5,6,7,8,9) \leftrightarrow (00,01,02,10,11,12,20,21,22)$$

then the subset  $S_{00}$  would have (000011011) as its vector representation. By considering the differences of elements of  $S_{00}$  and noting that no difference occurs more than twice, then by Corollary 7.8 no two translates of  $S_{00}$  will have more than two elements in common. Since each  $S_{ij}$  has four elements, the corresponding vector representations provide



nine vectors of weight four having at most two elements in common, and thus at least distance four from each other. Similarly, we can derive nine different subsets  $T_{ij}$  of order four, any two having at most two elements in common, by taking as elements of  $T_{ij}$  those four  $i'j'$  that are in the same row and column as  $ij$ . This provides another nine vectors of weight four at least distance four from each other. For example,  $T_{00} = \{01, 02, 10, 20\}$ . By considering the differences of elements of  $S_{00}$  and  $T_{00}$  and applying Proposition 7.7, it can be determined that any pairs of translates of  $S_{00}$  and  $T_{00}$  will have at most two elements in common. Thus we have eighteen vectors of weight four with minimum distance at least four between them. By adding the vector of all zeros and that of all ones, we have a noncyclic  $(9,4;20)$ -code. By deleting one coordinate, we get an  $(8,3;20)$ -code, proving that  $A(8,3) \geq 20$ . But by Wax's bound [27],  $A(8,3) \leq 20$ , and thus  $A(8,3) = 20$ .

As we have mentioned in the preceding section, a polynomial code is one which is both cyclic and linear, the name being motivated by the fact that a code with these properties has a polynomial representation. In particular, consider the factor ring  $R = \mathbb{Z}_2[X]/(X^n + 1)$  of  $2^n$  elements. Each residue class contains a polynomial of degree less than  $n$  which can be taken as its representative, and there is a one-to-one correspondence between these representatives and the elements of the vector space  $V_n$ ; hence a one-to-one correspondence between residue classes and vectors. More precisely, given  $\underline{a} = (a_{n-1}, a_{n-2}, \dots, a_0)$  of  $V_n$ , its polynomial representation is  $a(X) = a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \dots + a_0$ . Given a polynomial  $b(X)$  of degree greater than  $n$ , the polynomial of smallest degree in the same equivalence class can be found by dividing  $b(X)$  by  $X^n + 1$ , the remainder being the desired polynomial. Denote by  $\{a(X)\}$  the residue class of  $a(X)$ , where  $a(X)$  is always taken as the polynomial of smallest degree in the equivalence class.

Proposition 8.1. In the algebra of polynomials modulo  $X^n + 1$ , a subspace  $C$  is a cyclic subspace iff it is an ideal.

Proof. Assume  $C$  is an ideal in  $\mathbb{Z}_2[X]/(X^n + 1)$ . Then in  $\mathbb{Z}_2[X]/(X^n + 1)$ ,

$$\begin{aligned} X(a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \dots + a_0) &= a_{n-1}(X^n - 1) + a_{n-2}X^{n-1} + \dots + a_0X + a_{n-1} \\ &= a_{n-2}X^{n-1} + a_{n-3}X^{n-2} + \dots + a_0X + a_{n-1}. \end{aligned}$$

Thus if  $C$  is an ideal and  $a(X)$  is an element of  $C$ , then  $Xa(X)$  is in  $C$  and since  $Xa(X)$  is the cyclic shift of  $a(X)$ ,  $C$  is a cyclic subspace.

Next assume that  $C$  is a cyclic subspace. Then for  $a(X)$  in  $C$ ,  $Xa(X)$  is also in  $C$  and so for any  $i$ ,  $(X)^i a(X)$  is in  $C$ . Then since  $C$  is a subspace, any linear combination

$$a_{n-1}X^{n-1}(a(X)) + a_{n-2}X^{n-2}(a(X)) + \dots + a_0(a(X)) = (a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \dots + a_0)(a(X))$$

is in  $C$ . Then  $C$  is an ideal. QED

Let  $g(X)$  be the monic polynomial of smallest degree such that  $\{g(X)\}$  is in an ideal  $I$  in  $R$ . If  $f(X)$  is a polynomial of degree less than  $n$  that is divisible by  $g(X)$ , then  $\{f(X)\}$  is also in  $I$ . Conversely, if  $\{f(X)\}$  is in  $I$ , then  $f(X)$  is divisible by  $g(X)$ . Also, if  $g(X)$  is such a polynomial, then  $g(X)$  divides  $X^n + 1$  and every monic polynomial that divides  $X^n + 1$  generates a distinct ideal in  $Z_2[X]/(X^n + 1)$ . The polynomial  $g(X)$  is called the generator of the ideal.

From these remarks, we see that a polynomial code  $C$  is completely defined by a polynomial  $g(X)$  that divides  $X^n + 1$ , called the generating polynomial of  $C$ . As was the case with a general linear code, a polynomial code may also be expressed in terms of the null space of the ideal generated by the polynomial  $h(X)$  where  $h(X) = X^n + 1/g(X)$ . Clearly the polynomial  $h(X)$ , called the parity check polynomial of  $C$ , also divides  $X^n + 1$  and can be used to generate a code  $C'$ , called the dual code of  $C$ .

Let  $g(X)$  be a divisor of  $X^n + 1$  in  $Z_2[X]$  where  $\text{degree } g(X) = r$  so that  $X^n + 1 = g(X)h(X)$  for some polynomial  $h(X)$  of degree  $k$  where  $n = k + r$ .

Proposition 8.2. If  $g(X)$  is a divisor of  $f(X)$  in  $Z_2[X]/(X^n + 1)$ , then there is a unique polynomial  $m(X)$  of degree less than  $k$  such that  $f(X) = m(X)g(X)$ .

Proof. We know  $f(X) = m'(X)g(X)$  for some  $m'(X)$  in  $Z_2[X]/(X^n + 1)$  since  $g(X)$  divides  $f(X)$ . Then  $f(X) = m(X)g(X)$  also iff  $m'(X)g(X) = m(X)g(X)$  iff  $m'(X)g(X) \equiv m(X)g(X)$  modulo  $X^n + 1$  iff  $m'(X) \equiv m(X)$  modulo  $h(X)$ , where  $X^n + 1 = g(X)h(X)$ . But  $\deg h(X) = k$  and so the division algorithm assures us of a unique  $g(X)$  with degree less than  $k$ . QED

The construction of a polynomial code of length  $n$  and dimension  $k$  follows easily from the previous remarks. Take a generating polynomial  $g(X)$  of degree  $r$  which divides  $X^n + 1$  where  $n = k + r$ . The codewords will be elements of the ideal generated by  $g(X)$ . They will be elements of  $Z_2[X]/(X^n + 1)$  and the messages will be those elements of  $Z_2[X]/(X^n + 1)$  of degree less than  $k$ . The codewords will be multiples of the generating polynomial  $g(X)$ ; i.e. if  $f(X)$  is any polynomial of degree less than  $k$ , then the codeword  $c(X)$  is given by  $c(X) = f(X)g(X)$ . Clearly, these are  $2^k$  codewords since there are  $2^k$  possible messages.

As an example, consider  $Z_2[X]/(X^7 + 1)$ . In terms of its irreducible factors  $X^7 + 1 = (X + 1)(X^3 + X + 1)(X^3 + X^2 + 1)$  in  $Z_2$ . If  $g(X) = X^3 + X^2 + 1$ , let this correspond to 0001101 in  $V_7$ . Then  $Xg(X) = X^4 + X^3 + X$  corresponds to 0011010 in  $V_7$ ,  $X^2g(X) = X^5 + X^4 + X^2$  corresponds to 0110100, and  $X^3g(X) = X^6 + X^5 + X^3$  corresponds to 1101000. The rank of the ideal generated by  $g(X)$  is  $7 - \deg g(X) = 4$ . Thus  $g(X)$ ,  $Xg(X)$ ,  $X^2g(X)$  and  $X^3g(X)$  form a basis for the vector sub-



space of the ideal generated by  $g(X)$ . We may follow the same procedure as we did with general linear codes and take the corresponding basis vectors as the rows of a matrix  $G$ . Then

$$G = \begin{bmatrix} 001101 \\ 0011010 \\ 0110100 \\ 1101000 \end{bmatrix}$$

and  $G$  may be taken as a generating matrix for the code  $C$ . As we have noted,  $C$  is also the null space of the ideal generated by  $h(X) = (X + 1)(X^3 + X + 1) = X^4 + X^3 + X^2 + 1$ . Let  $h(X)$  correspond to 0011101,  $Xh(X)$  to 0111010, and  $X^2h(X)$  to 1110100. Because polynomial multiplication and inner product of vectors differ, then  $C$  is the null space of a matrix  $H$  with rows  $X^2h(X)$ ,  $Xh(X)$ ,  $h(X)$  with the order of the coordinates reversed. Then the parity check matrix  $H$  is given by

$$H = \begin{bmatrix} 0010111 \\ 0101110 \\ 1011100 \end{bmatrix}$$

where  $GH^T = 0$ . The message words for this code are polynomials of degree less than 4. In vector representation and with their corresponding coded form, they are

0000 $\leftrightarrow$ 0000000	1001 $\leftrightarrow$ 1100101
0001 $\leftrightarrow$ 1101000	1010 $\leftrightarrow$ 0111001
0010 $\leftrightarrow$ 0110100	0101 $\leftrightarrow$ 1110010
0100 $\leftrightarrow$ 0011010	0111 $\leftrightarrow$ 1000110
1000 $\leftrightarrow$ 0001101	1110 $\leftrightarrow$ 0100011
0011 $\leftrightarrow$ 1011100	1101 $\leftrightarrow$ 1111111
0110 $\leftrightarrow$ 0101110	1011 $\leftrightarrow$ 1010001
1100 $\leftrightarrow$ 0010111	1111 $\leftrightarrow$ 1001011

Since the code is linear, the minimum distance is given by the minimum weight of the nonzero words, namely 3. This code is equivalent to the Hamming  $(7,3;2^4)$ -code.

A polynomial code can also be specified in terms of the roots of its generating polynomial. The Bose-Chaudhuri-Hocquengham (BCH) codes defined following Theorem 8.4 are a class of codes specified in this manner. An easily implemented decoding procedure has been devised for them, making BCH codes quite important in a practical sense [1, Ch.12].

**Theorem 8.3.** [29] Let  $F$  be a field and  $\alpha$  a primitive  $n^{\text{th}}$  root of unity in some overfield of  $F$ . Let  $f(X)$  be a polynomial in  $F[X]$  of degree less than  $n$  and suppose that  $f(X)$  has  $d - 1$  successive powers of  $\alpha$  among its roots; i.e. for some integer  $t$ ,  $f(\alpha^{t+i}) = 0$  for  $i = 0, 1, \dots, d - 2$ . Then either  $f(X) = 0$  or  $f(X)$  has at least  $d$  nonzero coefficients.

**Proof.** Suppose  $f(X)$  has at most  $d - 1$  nonzero coefficients and let  $f(X) = c_1 X^{m_1} + c_2 X^{m_2} + \dots + c_{d-1} X^{m_{d-1}}$  where  $0 \leq m_1 < m_2 < \dots < m_{d-1} < n$ . Put  $\beta_1 = \alpha^{m_1}$ ,  $\beta_2 = \alpha^{m_2}$ , ...,  $\beta_{d-1} = \alpha^{m_{d-1}}$ . Then  $\beta_1, \beta_2, \dots, \beta_{d-1}$  are distinct and nonzero.

By hypothesis,

$$\begin{aligned} 0 = f(\alpha^{t+i}) &= c_1 \alpha^{m_1(t+i)} + c_2 \alpha^{m_2(t+i)} + \dots + c_{d-1} \alpha^{m_{d-1}(t+i)} \\ &= c_1 \beta_1^{t+i} + c_2 \beta_2^{t+i} + \dots + c_{d-1} \beta_{d-1}^{t+i} \quad \text{for } i = 0, 1, \dots, d-2. \end{aligned}$$

Equivalently we have

$$(c_1 \beta_1^t, c_2 \beta_2^t, \dots, c_{d-1} \beta_{d-1}^t) \begin{bmatrix} 1 & \beta_1 & \beta_1^2 & \dots & \beta_1^{d-2} \\ 1 & \beta_2 & \beta_2^2 & \dots & \beta_2^{d-2} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \beta_{d-1} & \beta_{d-1}^2 & \dots & \beta_{d-1}^{d-2} \end{bmatrix} = (0, 0, \dots, 0)$$

But since this  $(d-1) \times (d-1)$  matrix is nonsingular, then  
 $(c_1^{\beta_1^t}, c_2^{\beta_2^t}, \dots, c_{d-1}^{\beta_{d-1}^t}) = (0, 0, \dots, 0)$  and  $c_1 = c_2 = \dots = c_{d-1} = 0$ ; i.e.  
 $f(X)$  is the zero polynomial. QED

Recalling that for a linear code the minimum distance between codewords is at least equal to the minimum weight of the nonzero codewords and considering Theorem 8.3, we present without further proof

Theorem 8.4. Let  $\alpha$  be a primitive  $n^{\text{th}}$  root of unity in some overfield of  $Z_2$ . Let  $g(X)$  be a divisor of  $X^n + 1$  in  $Z_2[X]$  such that  $g(X)$  has  $d-1$  successive powers of  $\alpha$  among its roots. If  $C$  is the cyclic code with generating polynomial  $g(X)$  in  $Z_2[X]/(X^n + 1)$ , then  $C$  is an  $(n, d)$ -code.

An  $(n, d)$ -code  $C$  such as defined in Theorem 8.4 is called a BCH code. If  $n = 2^m - 1$  for some integer  $m$ , then  $C$  is a primitive BCH code; for any other odd  $n$ , the code is called nonprimitive. Furthermore the minimum distance determined by this construction is called the BCH distance (or designed distance) and may be less than the actual Hamming distance of the code under consideration.

Remark. Some interesting results on minimum distance, BCH distance, and the dimension of polynomial codes of lengths  $\leq 65$  have been tabulated by Chen [3] through the use of a computer. A good general discussion of BCH codes may be found in Peterson and Weldon [18].

The Reed-Muller (RM) codes are another class of polynomial codes specified in terms of the roots of the generating polynomial. The shortened  $r^{\text{th}}$  order Reed-Muller code  $C$  over  $GF(2)$  is the polynomial code

of length  $2^m - 1$  whose generating polynomial  $g(x)$  is given by

$$g(x) = \prod_j (x - \alpha^j)$$

$$0 \leq s(j) < m-r$$

$$0 \leq j < 2^m - 1$$

where  $s(j)$  is the number of digits in the binary expansion of  $j$  and  $\alpha$  is a primitive element in  $GF(2^m)$ . The  $r^{\text{th}}$  order Reed-Muller code over  $GF(2)$  is derived from  $C$  by appending a parity check digit to the shortened RM code, providing a code of length  $2^m$ .

Proposition 8.5. The  $r^{\text{th}}$  order RM code has minimum distance between codewords at least  $2^{m-r}$ .

Proof. For  $j = 1, 2, \dots, 2^{m-r} - 2$  we have  $s(j) < m - r$ . The result follows from Theorem 8.3. QED

Proposition 8.6. There are  $\sum_{i=0}^r \binom{m}{i}$  information symbols in the  $r^{\text{th}}$  order RM code.

Proof. The result follows easily from the fact that there are  $\binom{m}{i}$  integers  $j$  such that  $0 \leq j < 2^m$  and  $s(j) = i$ . QED

Letting  $R = \sum_{i=0}^r \binom{m}{i}$  the preceding two propositions clearly show that the  $r^{\text{th}}$  order Reed-Muller code is an  $(2^m, 2^{m-r}; 2^R)$ -code.

Remark. We note that the Reed-Muller codes may also be developed in terms of matrices. A good discussion may be found in Peterson and Weldon [18, p.125].

The Hamming codes are also representable in terms of polynomials, as shown in



Proposition 8.7. Let  $g(X)$  be a primitive binary polynomial of degree  $r$ ,  $n = 2^r - 1$ , and  $k = n - r$ . The  $k$  - dimensional polynomial code of length  $n$  with generating polynomial  $g(X)$  has minimum weight of its nonzero codewords equal to 3.

Proof. As we will consider both  $R = \mathbb{Z}_2[X]/(X^n + 1)$  and the field  $F = \mathbb{Z}_2[X]/(m(X))$ , we can avoid confusion by denoting the residue class of  $X$  modulo  $m(X)$  by  $\alpha \in F$  and retain  $X$  for  $X$  modulo  $X^n + 1$  in  $R$ . Also, by Lagrange's Theorem, since  $m(X)$  is an irreducible polynomial of degree  $r$ , then  $m(X)$  divides  $X^n + 1$ .

Consider  $f(X)$  in  $\mathbb{Z}_2[X]$ . Since  $m(X)$  divides  $X^n + 1$ , then  $f(X)$  will be divisible by  $m(X)$  in  $R$  iff  $m(X)$  divides  $f(X)$  in  $\mathbb{Z}_2[X]$ . But  $f(X) \equiv 0 \pmod{m(X)}$  iff  $f(\alpha) = 0$  in  $F$ . But then  $f(X)$  is a codeword ( $f(X)$  is divisible by  $m(X)$  in  $R$ ) iff  $f(\alpha) = 0$  in  $F$ .

We must show that no nonzero codewords are of weight less than 3. Suppose that  $X^t$  were a codeword. But then  $\alpha^t = 0$  in  $F$ , a contradiction. Next suppose that  $X^t + X^s$  were a codeword, for  $0 \leq s < t < n$ . Then  $\alpha^t + \alpha^s = 0$  and  $\alpha^t = \alpha^s$  in  $F$ . This contradicts the fact that  $m(X)$  is primitive,  $\alpha$  being a primitive element in  $F$ . QED

As an example, consider the case  $n = 7$  (hence  $r = 3$ ,  $k = 4$ ). A generating polynomial is the primitive polynomial  $X^3 + X + 1$ . Given a message  $(a_0, a_1, a_2, a_3)$  its corresponding codeword is found by completing the multiplication of  $(a_3X^3 + a_2X^2 + a_1X + a_0)(X^3 + X + 1)$ . For example, the message 0011 has  $(X + 1)(X^3 + X + 1) = X^4 + X^3 + X^2 + 1$ , or 0011101 as its corresponding codeword.

There is another construction of polynomial codes from the quadra-

tic residues. If  $n$  is a prime of the form  $8m \pm 1$ , then  $g^i$  is a quadratic residue iff  $2g^i, 4g^i, 8g^i, \dots$  are also. Thus the set of quadratic residues consists of one or more complete cycle sets. This is also true for the nonresidues. Then  $x^n + 1$  factors into  $(x + 1)g_r(x)g_n(x)$  where the roots of  $g_r(x)$  are the quadratic residues and  $g_n(x)$  has the nonresidues as its roots. Polynomial codes called quadratic residue codes may be constructed by taking  $g_r(x)$ ,  $(x + 1)g_r(x)$ ,  $g_n(x)$ , and  $g_n(x)(x + 1)$  as the generating polynomials. We note that the Golay (23,7)-code can be constructed in this way [18,p.256].

### 9. A Class of Nonlinear Codes Derived from Polynomials

Nordstrom and Robinson [17] constructed an optimal nonlinear code  $C$  having length 15, minimum distance at least 5, and 256 codewords.

The code is systematic with eight information positions  $X_0, X_1, \dots, X_7$  and seven check digits denoted by  $Y_0, Y_1, \dots, Y_6$ . Define  $Y_0$  by

$$Y_0 = \begin{aligned} &X_7 \oplus X_6 \oplus X_0 \oplus X_1 \oplus X_3 \\ &\oplus (X_0 \oplus X_4) (X_1 \oplus X_2 \oplus X_3 \oplus X_5) \\ &\oplus (X_1 \oplus X_2) (X_3 \oplus X_5) \end{aligned}$$

where  $\oplus$  denotes addition modulo 2. The remaining  $Y_i$  are found by cyclically shifting  $X_0$  through  $X_6$ ; i.e. for  $Y_j$  substitute  $X_{i+j(\text{mod } 7)}$  for  $X_i$  where  $i = 0, 1, \dots, 6$  for each  $j$  where  $j = 0, 1, \dots, 6$ . They calculated that there were 256 codewords and observed that the minimum distance between them was 5, proving that  $A(15, 5) \geq 256$ . But Johnson's bound provides  $A(15, 5) \leq 256$  so that the code being considered is optimal. In [20], Preparata presented a polynomial representation for the Nordstrom-Robinson code and formally proved its weight distribution and distance structure.

Nordstrom and Robinson further raised the question as to whether or not their  $(15, 5; 256)$ -code was a member of a general class of nonlinear codes, inspiring Preparata to discover a class of optimal nonlinear double-error-correcting codes. He presented the following proposition, the proof of which may be found in [21].

**Proposition 9.1.** For even integers  $m \geq 4$ , there exists an  $(2^m - 1, 5; 2^{2^m - 2m})$ -code.

This class of Preparata codes is important as they have straightforward encoding and decoding algorithms. They are also important because they contain twice as many codewords as the corresponding BCH  $(2^m-1, 5; 2^{2^m-1-2^m})$ -codes; in fact, they are optimal by Johnson's bound, as will be shown in Section 13.



# 10. Constructions Using Hadamard Matrices, Conference Matrices and Combinatorial Designs

Several codes have been constructed by means of combinatorial designs, often providing excellent lower bounds for  $A(n,d)$ .

For example, by considering the intersection of five lines in a plane, Golay [8] determined that  $A(10,3) \geq 68$ . He furthermore determined from the results of his construction that  $A(11,3) \geq 136$ ,  $A(9,3) \geq 38$  and  $A(8,3) \geq 20$ . His observations were later improved to show  $A(10,3) \geq 72$  and  $A(11,3) \geq 144$  [13].

Sloane and Whitehead [26] employed Steiner systems in another approach to the same problem. A Steiner system, denoted by  $S(t,k,v)$ , is a set of  $v$  points together with a class of subsets (called blocks) of size  $k$  such that given these blocks of size  $k$ , every set of  $t$  points is contained in exactly one block. Consider the Steiner system  $S(5,6,12)$  of 132 blocks, a set of twelve points such that every set of five points is contained in one block of size six. But then these blocks can have at most four points in common so that there are two points in each block that are not in the other. By representing each block as a vector of length twelve and weight six, these vectors can have at most four coordinates in common so that they must be at least distance four from each other, and these vectors form an  $(12,4;132)$ -code in which all codewords have weight six. Deleting the first coordinate, we have a cyclic  $(11,3;132)$ -code with 66 words of weight five and 66 words of weight six. By adding five words of weight two which are coordinatewise disjoint, their five complements of weight nine, and the word  $(000000000001)$  and its complement, we have an  $(11,3;144)$ -code  $C_{11}$ . Half the words are of even

weight and half are of odd weight. Taking the codewords that are of even weight, we get an  $(11,4;72)$ -code which contains a cyclic set of 66 words of weight six. Deleting a coordinate provides an  $(10,3;72)$ -code  $C_{10}$ , having five words of weight two, 36 words of weight five, thirty of weight six, and one of weight ten. By deleting one coordinate from the 36 words of weight five and adding the vector of all zeros and the vector of all ones, we have an  $(9,3;38)$ -code  $C_9$ . Among its codewords are 18 words of weight four. By deleting a coordinate from these and adding the vector of all zeros and that of all ones, we get an  $(8,3;20)$ -code  $C_8$ . Wax's bound [27] gives  $A(8,3) \leq 20$  so that by the above construction,  $A(8,3) = 20$ . The other codes generated by this construction are not known to be optimal, but do give better results than any linear code.

Another code construction is that developed from the theory of Hadamard matrices. A Hadamard matrix is an orthogonal  $n \times n$  matrix whose coordinates are the real numbers  $+1$  and  $-1$ ; i.e. its rows are orthogonal  $n$ -tuples. It is known that Hadamard matrices exist only when  $n = 2$  and  $n = 4t$  where  $t$  is a positive integer [2].

Proposition 10.1. If there exists an  $n \times n$  Hadamard matrix, then there exists a binary code of length  $n$  with  $2n$  codewords and minimum distance at least  $\frac{n}{2}$ ; i.e. if there is an  $n \times n$  Hadamard matrix, then there exists an  $(n, \frac{n}{2}; 2n)$ -code (which is optimal by Plotkin's bound).

Proof. Let  $H$  be an  $n \times n$  Hadamard matrix. Let  $S = \{\pm r_1, \pm r_2, \dots, \pm r_n\}$  be the set of  $2n$  vectors where  $r_i$  is a row of  $H$ . In each of these vectors, change the  $+1$ 's to zeros and the  $-1$ 's to ones. This gives a set of  $2n$  vectors of length  $n$ . Since corresponding coordinates of  $r_i$  and  $-r_i$

are different, the distance between  $\underline{r}_i$  and  $-\underline{r}_i$  is  $n$ .

Since  $\pm \underline{r}_i$  and  $\pm \underline{r}_j$  are orthogonal if  $i \neq j$ , they must be the same in precisely half of the coordinates and differ in the other half and so are at distance  $\frac{n}{2}$ . But then the minimum distance between any two vectors is at least  $\frac{n}{2}$ . QED.

Remark [23]. If  $n = 2^k$  for some integer  $k$ , then the resulting  $(2^k, 2^{k-1}; 2^{k+1})$ -code is a linear first order Reed-Muller code. For those  $n$  which are not powers of 2, the Hadamard codes are nonlinear.

The preceding construction involving Hadamard matrices can also be approached in terms of balanced incomplete block designs. A balanced incomplete block design is an arrangement of  $v$  objects into  $b$  sets such that each set contains exactly  $k$  different objects, each object occurs in exactly  $r$  different sets, and any pair of objects occurs in exactly  $\lambda$  different sets. The integers  $v, b, r, k, \lambda$  are the parameters of the design and satisfy  $bk = vr$  and  $\lambda(v-1) = r(k-1)$ . The design is said to be symmetrical if  $b = v$  so that also  $k = r$ . Bose and Shrikhande [2] and others have proven the equivalence of Hadamard matrices and block designs for specific parameters. We present without proof Proposition 10.2, which may be found in [2].

Proposition 10.2 The following statements are equivalent:

- (i)  $A(4t, 2t) = 8t$ ; i.e. there exists an  $(4t, 2t; 8t)$ -code;
- (ii)  $A(4t-1, 2t) = 4t$ ; i.e. there exists an  $(4t-1, 2t; 4t)$ -code;
- (iii) A symmetric balanced incomplete block design with parameters  $v = b = 4t-1$ ,  $r = k = 2t-1$ ,  $\lambda = t-1$  exists;
- (iv) A Hadamard matrix of order  $4t$  exists.

Continuing the discussion of code construction involving Hadamard

AD-A047 072

OHIO STATE UNIV COLUMBUS DEPT OF MATHEMATICS  
COMBINATORIAL SYSTEMS.(U)  
MAR 73 D K RAY-CHAUDHURI

F/G 9/4

UNCLASSIFIED

2 OF 2  
AD  
A047 072

N00014-67-A-0232-0016  
NL





matrices, Levenshtein [15] derives nonlinear codes from these matrices and further shows that the codes he constructs are optimal by Plotkin's bound for all  $n \leq 2d$ . He first defines a matrix to be regular if it is of order  $n$ , is composed of zeros and ones, and has the property that the distance between any two rows is  $\frac{n}{2}$ . A regular matrix of order  $n$  exists iff there exists a Hadamard matrix of the same order (cf. the matrix construction in the proof of Proposition 10.1).

Levenshtein's construction is based on the operations of adjunction and extension of matrices, where the extension of a matrix  $A$   $r$  times, denoted as  $rA$ , is defined as the result of consecutive adjunctions of  $r$  matrices  $A$  and adjunction is defined by: Given

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n_1} \\ a_{21} & a_{22} & \dots & a_{2n_1} \\ \vdots & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \\ a_{k_1 1} & a_{k_1 2} & \dots & a_{k_1 n_1} \end{bmatrix} \quad B = \begin{bmatrix} b_{11} & b_{12} & \dots & b_{1n_2} \\ b_{21} & b_{22} & \dots & b_{2n_2} \\ \vdots & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \\ b_{k_2 1} & b_{k_2 2} & \dots & b_{k_2 n_2} \end{bmatrix}$$

then the adjunction of  $A$  and  $B$ , denoted by  $A \oplus B$ , is defined by

$$A \oplus B = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n_1} & b_{11} & b_{12} & \dots & b_{1n_2} \\ a_{21} & a_{22} & \dots & a_{2n_1} & b_{21} & b_{22} & \dots & b_{2n_2} \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{k_1 1} & a_{k_1 2} & \dots & a_{k_1 n_1} & b_{k_1 1} & b_{k_1 2} & \dots & b_{k_1 n_2} \end{bmatrix}$$

where  $k = \min(k_1, k_2)$ . He then constructs a code from two others whose existence is guaranteed by results such as Proposition 10.1 and Proposition 10.2. By taking a matrix  $A$  whose rows form an  $(n_1, d_1; A_1)$ -code and a matrix  $B$  whose rows form an  $(n_2, d_2; A_2)$ -code construct a matrix  $aA \oplus bB$

whose rows form an  $(an_3, d_3; A_3)$ -code where  $n_3 = an_1 + bn_2$ ,  $d_3 = ad_1 + bd_2$ ,  $A_3 = \min(A_1, A_2)$  and  $a$  and  $b$  are nonnegative integers. Using Plotkin's upper bound on  $A(n, d)$ , Levenshtein's results provide

Proposition 10.3. If  $d$  is odd, then  $A(n, d) = 2\left[\frac{d+1}{2d+1-n}\right]$  for  $2d+1 > n \geq d$  and  $A(n, d) = 2(n+1)$  for  $2d+1 = n$ .

Proof. See Levenshtein.

A family of good nonlinear codes have also been derived from conference matrices. An  $n \times n$  conference matrix  $T_n = (t_{ij})$  satisfies the properties that  $t_{ii} = 0$ ,  $t_{ij} = +1$  or  $-1$  for  $i \neq j$  and  $T_n T_n' = (n-1)I_n$  where  $I_n$  is the  $n \times n$  unit matrix. Sloane and Seidel [25] have noted that the necessary conditions for a real symmetric conference matrix  $T_{q+1}$  to exist are  $q = 4k+1$  and  $q = a^2 + b^2$  where  $a$ ,  $b$  and  $q$  are integers. They further prove that the existence of an  $n \times n$  conference matrix  $T_n$  is equivalent to the existence of a nonlinear  $(n-1, \frac{1}{2}(n-2); 2n)$ -code. One code obtainable in this manner is a  $(9, 4; 20)$ -code from which the optimal  $(8, 3; 20)$ -code can be derived.

In the proof of Proposition 4.4, Plotkin developed a code of length  $2n$  by concatenating codewords from two codes of length  $n$ ; i.e. by appending the codeword from one onto the codeword of the other. This method has been successfully refined by both Sloane and Whitehead [26] and Liu, Ong, and Ruth [16]. An example will be noted in this section illustrating how this method has provided improved lower bounds for  $A(n,d)$ . We present Sloane and Whitehead first as it appeared first in the literature.

Sloane and Whitehead construct an  $(2n, d_1; A_1 A_2)$ -code  $C$  by combining an  $(n, d_1; A_1)$ -code  $C_1$  and an  $(n, d_2; A_2)$ -code  $C_2$  where  $d_2 = \frac{1}{2}(d_1 + 1)$ . A codeword in  $C$  is determined by adding an arbitrary codeword of  $C_1$  to an arbitrary codeword of  $C_2$  and appending the codeword of  $C_2$  to the result. More formally,

$C = C_1 \oplus C_2 = \{ \underline{a} \oplus \underline{b} : \underline{a} \in C_1, \underline{b} \in C_2 \}$  where  $\oplus$  is defined in the following way: If  $\underline{a} = (a_1, a_2, \dots, a_n)$  and  $\underline{b} = (b_1, b_2, \dots, b_n)$ , then  $\underline{a} \oplus \underline{b} = (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n, b_1, b_2, \dots, b_n)$ , where  $+$  is addition modulo 2. The resulting code  $C$  is clearly of length  $2n$ . It remains to be shown that  $d_1$  is the minimum distance between codewords of  $C$  and that it contains  $A_1 A_2$  codewords. Since each choice of codewords  $\underline{a}$  of  $C_1$  and  $\underline{b}$  of  $C_2$  will produce different results for  $\underline{a} \oplus \underline{b}$ , there are  $A_1 A_2$  codewords in  $C$ . If  $\underline{a}_1 \neq \underline{a}_2$ , then  $\underline{a}_1$  and  $\underline{a}_2$  differ in  $d_1$  coordinates and thus so would  $\underline{a}_1 \oplus \underline{b}_1$  and  $\underline{a}_2 \oplus \underline{b}_2$  for all  $\underline{b}_1$  and  $\underline{b}_2$  in  $C_2$ . If  $\underline{a}_1 = \underline{a}_2$  and  $\underline{b}_1 \neq \underline{b}_2$ , then the distance between the  $a_i + b_i$  portions of  $\underline{a}_1 \oplus \underline{b}_1$  and  $\underline{a}_2 \oplus \underline{b}_2$  would be at least  $d_2$ , as would the distance between the  $b_i$  coordinates, so that the distance between  $\underline{a}_1 \oplus \underline{b}_1$  and

$\frac{a}{2} \oplus \frac{b}{2}$  would be at least  $2d_2 = 2(\frac{1}{2}(d_1 + 1)) = d_1 + 1 > d_1$ . Thus we have

Theorem 11.1. If  $C_1$  is an  $(n, d_1; A_1)$ -code and  $C_2$  is an  $(n, d_2; A_2)$ -code where  $d_2 = \frac{1}{2}(d_1 + 1)$ , then  $C = C_1 \oplus C_2$  is an  $(2n, d_1; A_1 A_2)$ -code.

The next proposition is a result useful in constructing codes from other codes. The proof is obvious and is not included.

Proposition 11.2. Given an  $(n, d)$ -code  $C$ , then the addition of a parity check digit causing every codeword to have even (or odd) parity produces an  $(n + 1, d)$ -code.

By the Sloane and Whitehead method, combining the  $(8, 3; 20)$ -code of Section 10 with a single parity check  $(8, 2; 2^7)$ -code produces an  $(16, 3; \frac{5}{4} (2048))$ -code, better than any linear result previously known. Employing Proposition 11.2, we can derive an  $(9, 4; 20)$ -code from the  $(8, 3; 20)$ -code. Combining this with an  $(9, 2; 2^8)$ -code gives an  $(18, 4; \frac{5}{4} (2^{12}))$ -code and so an  $(17, 3; \frac{5}{4} (2^{12}))$ -code. From the  $(9, 3; 38)$ -code of Section 10 and an  $(9, 2; 2^8)$ -code we get an  $(18, 3; \frac{19}{16} (2^{13}))$ -code. From these and other observations, Sloane and Whitehead note the next proposition without proof.

Proposition 11.3. For any block length  $n$  such that  $2^m \leq n \leq 3 \cdot 2^{m-1}$ , there exists a nonlinear  $(n, 3; \lambda 2^{n-m-1})$ -code, where  $\lambda = \frac{5}{4}$ ,  $\frac{19}{16}$ , or  $\frac{9}{8}$  according as the binary expansion of  $n$  begins with 1000, 1001, or 101.



Liu, Ong and Ruth also present the preceding proposition without proof. We proceed with their construction, similar to the Sloane and Whitehead method, but more general in that the results may not be linear and the minimum distance of the resulting Liu-Ong-Ruth code may be an improvement over the minimum distance of either original code.

The general construction of Liu, Ong, and Ruth begins with a systematic  $(n, d_1; 2^k)$ -code  $C_1$  which may or may not be linear. Without loss of generality, choose  $C_1$  such that the first  $k$  positions of the codewords are all of the  $2^k$  possible  $k$ -tuples. Consider  $n$ -tuples of the form  $(0^k, \underline{y})$  where  $\underline{y}$  is an  $(n - k)$ -tuple; i.e. the  $n$ -tuples being considered have zeros in the first  $k$  coordinates. Since the number of these  $n$ -tuples is determined by the number of possible  $\underline{y}$ 's, there are  $2^{n-k}$  of them. Denote these  $n$ -tuples by  $\underline{x}_1, \underline{x}_2, \dots, \underline{x}_{2^{n-k}}$ . Let  $U(\underline{x})$  be the translate of  $C_1$  by  $\underline{x}$ ; i.e.  $U(\underline{x}) = \{\underline{x} + \underline{a} : \underline{a} \in C_1\}$ .

Proposition 11.4. The set of all vectors of  $V_n$  is partitioned into  $2^{n-k}$  disjoint subsets  $U(\underline{x}_1), U(\underline{x}_2), \dots, U(\underline{x}_{2^{n-k}})$  corresponding to the  $n$ -tuples  $\underline{x}_1, \underline{x}_2, \dots, \underline{x}_{2^{n-k}}$ . The distance between any two vectors in any given translate is at least  $d_1$ .

Proof. Since  $\underline{x} + \underline{a}_1 \neq \underline{x} + \underline{a}_2$  for distinct  $\underline{a}_1, \underline{a}_2$  in  $C_1$ , then every subset  $U(\underline{x})$  has exactly  $2^k$  distinct  $n$ -tuples. We must show that  $\underline{x}_1 + \underline{a}_1 \neq \underline{x}_j + \underline{a}_2$  for  $\underline{x}_1 \neq \underline{x}_j$ . If  $\underline{a}_1 = \underline{a}_2$ , then clearly  $\underline{x}_1 + \underline{a}_1 \neq \underline{x}_j + \underline{a}_2$  when  $\underline{x}_1 \neq \underline{x}_j$ . If  $\underline{a}_1 \neq \underline{a}_2$ , then the first  $k$  digits of  $\underline{a}_1$  are different from the first  $k$  coordinates of  $\underline{a}_2$  by our choice of  $C_1$ . Since the first  $k$  coordinates in both  $\underline{x}_1$  and  $\underline{x}_j$  are all zeros, the first  $k$  coordinates

of  $\underline{x}_i + \underline{a}_1$  must be different from the first  $k$  coordinates of  $\underline{x}_j + \underline{a}_2$ . Thus  $\underline{x}_i + \underline{a}_1 \neq \underline{x}_j + \underline{a}_2$  and the subsets  $U(\underline{x})$  are disjoint. Given any two vectors  $\underline{x} + \underline{a}_1$  and  $\underline{x} + \underline{a}_2$  in  $U(\underline{x})$  for arbitrary  $\underline{x}$ , their distance is equal to  $\Delta(\underline{a}_1, \underline{a}_2)$  which is at least  $d_1$ . QED

Using this result, the  $2^{n-k}$  translates of  $C_1$  can be used to partition the set of all  $n$ -tuples. Next take an  $(n, d_2; 2^{n-k})$ -code  $C_2$  and assign to each translate  $U(\underline{x})$  a unique codeword of  $C_2$ . We can now construct a code  $C$  of length  $2n$  with  $2^n$  codewords. Let  $\underline{x}$  be any of the  $2^n$  vectors of  $V_n$  and let  $f(\underline{x})$  denote the codeword of  $C_2$  that is assigned to the translate containing  $\underline{x}$ . The codeword in  $C$  is derived from the concatenation of the two vectors  $\underline{x}$  and  $\underline{x} + f(\underline{x})$ , denoted by  $(\underline{x}, \underline{x} + f(\underline{x}))$  where  $+$  is coordinatewise addition modulo 2 and by concatenation we mean appending the vector  $\underline{x} + f(\underline{x})$  onto the vector  $\underline{x}$ . The resulting code may or may not be linear.

For example, let  $C_1 = \{000, 111, 011, 100\}$  and  $C_2 = \{000, 010\}$ . The translates of  $C_1$  and the assignment of codewords of  $C_2$  are shown by

TRANSLATES OF $C_1$				ASSIGNMENT
000	111	011	100	000
011	110	010	101	010

where each row on the left is a translate. Then the codewords in  $C$  are given by

INFORMATION WORD (ELEMENTS OF $V_3$ )	CODEWORD OF $C$	
000	000	000
001	001	011
010	010	000
100	100	100
011	011	011
101	101	111
110	110	100
111	111	111

Theorem 11.5. The code  $C$  that is constructed from the  $(n, d_1; 2^k)$ -code  $C_1$  and the  $(n, d_2; 2^{n-k})$ -code  $C_2$  is an  $(2n, d; 2^n)$ -code where  $d \geq \min(2d_1, d_2)$ .

Proof. Clearly  $C$  is a code of length  $2n$  by construction. There are  $2^n$  codewords in  $C$  since all  $2^n$  vectors of  $V_n$  are allowed in construction. We must show  $d \geq \min(2d_1, d_2)$ .

Let  $(\underline{x}, \underline{x} + f(\underline{x}))$  and  $(\underline{y}, \underline{y} + f(\underline{y}))$  be two codewords in  $C$ .

Case 1. Suppose  $\underline{x}$  and  $\underline{y}$  are in the same translate of  $C_1$ .

Then  $f(\underline{x}) = f(\underline{y})$  and

$$\Delta[(\underline{x}, \underline{x} + f(\underline{x})), (\underline{y}, \underline{y} + f(\underline{y}))] = \Delta(\underline{x}, \underline{y}) + \Delta(\underline{x}, \underline{y}) \geq 2d_1.$$

Case 2. Suppose  $\underline{x}$  and  $\underline{y}$  are not in the same translate of  $C_1$ .

Then  $f(\underline{x}) \neq f(\underline{y})$  and

$$\begin{aligned} \Delta[(\underline{x}, \underline{x} + f(\underline{x})), (\underline{y}, \underline{y} + f(\underline{y}))] &= \Delta(\underline{x}, \underline{y}) + \Delta(\underline{x} + f(\underline{x}), \underline{y} + f(\underline{y})) \\ &\geq \Delta(f(\underline{x}), f(\underline{y})) = d_2. \end{aligned}$$

Therefore  $d \geq \min(2d_1, d_2)$ . QED

Remark. Note that  $\min(2d_1, d_2)$  is only a lower bound on the minimum distance  $d$  of  $C$ . If  $2d_1 \leq d_2$ , then  $d = 2d_1$ ; but if  $2d_1 > d_2$ , then  $\min(2d_1, d_2)$  is only a lower bound for  $d$  [16]. The distance may be improved by a more careful assignment of codewords of  $C_2$  to translates of  $C_1$ , which is possible since complete freedom is allowed in the assignment.

Remark. If  $C_1$  were a linear code, the codewords of  $C_2$  could be assigned to the  $2^{n-k}$  cosets of  $C_1$ .

The Liu-Ong-Ruth construction can also be employed when  $C_2$  does not have  $2^{n-k}$  codewords. Suppose then that  $|C_2| = m$ . If  $m < 2^{n-k}$ , select arbitrary  $m$  translates of  $C_1$  and assign them to distinct code-



words of  $C_2$ . Then using only those vectors  $\underline{x}$  of  $V_n$  that appear in the  $m$  translates selected, encode  $\underline{x}$  as  $(\underline{x}, \underline{x} + f(\underline{x}))$  where  $f(\underline{x})$  is again the codeword of  $C_2$  assigned to the translate of  $C_1$  containing  $\underline{x}$ . The resulting code  $C$  is an  $(2n, d; m2^k)$ -code where  $d \geq \min(2d_1, d_2)$ . If  $m > 2^{n-k}$ , let  $m = r2^{n-k}$ . Then assign to each translate of  $C_1$   $r$  distinct codewords of  $C_2$ . Look at a set  $R$  of  $r$  distinct vectors of  $V_n$ . Consider a one-to-one correspondence between the vectors in  $R$  and the codewords assigned to each translate of  $C_1$ . Let  $(\underline{x}, \underline{y})$  be an information word where  $\underline{x}$  is any vector in  $V_n$  and  $\underline{y}$  is a vector in  $R$ . Then  $(\underline{x}, \underline{y})$  will be encoded as  $(\underline{x}, \underline{x} + f(\underline{x}, \underline{y}))$  where  $f(\underline{x}, \underline{y})$  denotes the vector in  $C_2$  that is assigned to the translate containing  $\underline{x}$  and is in correspondence with  $\underline{y}$ . The result is an  $(2n, d; r2^n)$ -code where  $d \geq \min(2d_1, d_2)$ .

To demonstrate that freedom of assignment produces good results, consider the example presented by Liu, Ong, and Ruth. Taking both  $C_1$  and  $C_2$  to be the  $(8, 4; 2^4)$ -code obtained by appending a parity check digit to the cyclic  $(7, 3; 2^4)$ -code generated by the polynomial  $x^3 + x + 1$ , and by careful assignment of codewords of  $C_2$  to the cosets of  $C_1$ , they construct an  $(16, 6; 2^8)$ -code which provides an  $(15, 5; 2^8)$ -code after deleting any one of the sixteen coordinates. This result also proves that  $A(15, 5) = 256$  since Johnson's results (see Section 13) show  $A(15, 5) \leq 256$ . By comparison, the best linear code only gives  $A(15, 5) \geq 128$ .

As another example, Liu, Ong, and Ruth take a primitive element  $\alpha$  in  $GF(2^{m-1})$  and consider the  $(m-3)^{rd}$  order Reed-Muller codes,  $C_1$  and  $C_2$ , of length  $2^{m-1}$  obtained by appending a parity check digit to the polynomial code generated by  $g(X) = \prod_{j=0}^{m-2} (X - \alpha^{2^j})$ . In this case,  $C_1$



and  $C_2$  are both  $(2^{m-1}, 4; 2^{2^{m-1}-m})$ -codes. By carefully assigning  $2^{2^{m-1}-2m}$  codewords in  $C_2$  to each of the  $2^m$  cosets of  $C_1$ , they construct an  $(2^m, 6; 2^{2^m-2m})$ -code  $C$ . To illustrate the value of this construction, when  $m = 5$  the resulting  $(32, 6; 2^{22})$ -code provides the best known lower bound for  $A(32, 6)$  ( $=A(31, 5)$ ). For details of the assignment of codewords to cosets, see [16].

## 12. Some Other Important Code Constructions

There are other methods for combining codes to form other codes in addition to those demonstrated in the preceding section, many of which provide the best known lower bounds for  $A(n,d)$  for certain values of  $n$  and  $d$ . We first present some of those given by Sloane, Reddy and Chen [24].

Construction X. This construction begins with an  $(n_1, d_1; A_1)$ -code  $C_1$  and an  $(n_1, d_2; A_2 = bA_1)$ -code  $C_2$  where  $C_2$  is the union of  $b$  disjoint cosets of  $C_1$ ; i.e.  $C_2 = (\underline{x}_1 + C_1) \cup (\underline{x}_2 + C_1) \cup \dots \cup (\underline{x}_b + C_1)$  for some set of vectors  $S = \{\underline{x}_1, \underline{x}_2, \dots, \underline{x}_b\}$ . Next take any  $(n_3, d_3; b)$ -code  $C_3$  and consider a permutation  $\pi$  of  $\{1, 2, \dots, b\}$ . We can define a one-to-one mapping  $m$  from  $S$  onto  $C_3$  by  $m: \underline{x}_i \mapsto \underline{y}_{\pi(i)}$  where  $\underline{y}_{\pi(i)}$  is a codeword of  $C_3$ . Let  $(\underline{x}, \underline{y})$  denote the usual vector concatenation and define  $(S, \underline{y})$  by  $(S, \underline{y}) = \{(\underline{x}_i, \underline{y}) : \underline{x}_i \in S\}$ . The new code  $C_4$  is defined by  $(\underline{x}_1 + C_1, \underline{y}_{\pi(1)}) \cup (\underline{x}_2 + C_1, \underline{y}_{\pi(2)}) \cup \dots \cup (\underline{x}_b + C_1, \underline{y}_{\pi(b)})$ ; i.e.  $C_2$  is divided into cosets of  $C_1$  and a different codeword of  $C_3$  is attached to each coset.

Theorem 12.1.  $C_4$  is an  $(n_1 + n_3, d_4; A_2)$ -code where  $d_4 = \min\{d_1, d_2 + d_3\}$ .

Proof. Clearly  $C_4$  has block length  $n_1 + n_3$  and  $A_2$  codewords. We must show that the minimum distance between codewords is at least  $\min\{d_1, d_2 + d_3\}$ . Let  $\underline{c}_1 = (\underline{x}, \underline{y})$  and  $\underline{c}_2 = (\underline{x}', \underline{y}')$  be distinct codewords of  $C_4$ .

Case 1. Suppose  $\underline{x}$  and  $\underline{x}'$  belong to the same coset of  $C_1$ . Then

$$\underline{y} = \underline{y}' \text{ and } \Delta(\underline{c}_1, \underline{c}_2) = \Delta(\underline{x}, \underline{x}') \geq d_1.$$

Case 2. Suppose  $\underline{x}$  and  $\underline{x}'$  belong to different cosets of  $C_1$ . Then  $\Delta(\underline{x}, \underline{x}') \geq d_2$  and  $\Delta(\underline{y}, \underline{y}') \geq d_3$  giving  $\Delta(\underline{c}_1, \underline{c}_2) \geq d_2 + d_3$ .

The result follows easily. QED

Construction X4. This construction is a generalization of construction X and forms a code from four other codes. Take an  $(n_1, d_1; A_1)$ -code  $C_1$ , an  $(n_1, d_2; A_2 = bA_1)$ -code  $C_2$ , an  $(n_3, d_1; A_3)$ -code  $C_3$  and an  $(n_3, d_4; A_4 = bA_3)$ -code  $C_4$  where  $C_2$  is the union of  $b$  disjoint cosets of  $C_1$  and  $C_4$  is the union of  $b$  disjoint cosets of  $C_3$ ; i.e.  $C_2 = (\underline{x}_1 + C_1) \cup (\underline{x}_2 + C_1) \cup \dots \cup (\underline{x}_b + C_1)$  and  $C_4 = (\underline{y}_1 + C_3) \cup (\underline{y}_2 + C_3) \cup \dots \cup (\underline{y}_b + C_3)$  for some sets of vectors  $S_1 = \{\underline{x}_1, \underline{x}_2, \dots, \underline{x}_b\}$  and  $S_2 = \{\underline{y}_1, \underline{y}_2, \dots, \underline{y}_b\}$ . Again let  $\Pi$  be any permutation of  $\{1, 2, \dots, b\}$  and define a one-to-one mapping  $m$  from  $S_1$  onto  $S_2$ . Further define  $S_1 \times S_2$  to be the set of all possible concatenations  $(\underline{x}_i, \underline{y}_j)$  where  $\underline{x}_i \in S_1$  and  $\underline{y}_j \in S_2$ . The new code  $C_5$  is defined by  $C_5 = \bigcup_{i=1}^b (\underline{x}_i + C_1) \times (\underline{y}_{\Pi(i)} + C_3)$ ; i.e. the vectors of the  $i^{\text{th}}$  coset of  $C_1$  (codewords of  $C_2$ ) are concatenated in every possible way with the vectors of the  $\Pi(i)^{\text{th}}$  coset of  $C_3$  (codewords of  $C_4$ ).

Proposition 12.2.  $C_5$  is an  $(n_1 + n_3, d_5; A_2 A_3)$ -code where  $d_5 = \min \{d_1, d_2 + d_4\}$ .

Proof. Clearly  $C_5$  has block length  $n_1 + n_3$  and  $bA_1 A_3 = A_2 A_3$  codewords. We must show that the minimum distance between codewords is at least  $\min \{d_1, d_2 + d_4\}$ . Let  $\underline{c}_1 = (\underline{x}, \underline{y})$  and  $\underline{c}_2 = (\underline{x}', \underline{y}')$  be distinct codewords of  $C_5$ . Note that if  $\underline{x}$  and  $\underline{x}'$  are in the same coset of  $C_1$ , then  $\Delta(\underline{x}, \underline{x}') \geq d_1$ , the minimum distance of  $C_1$ , while if they are

in different cosets of  $C_1$ , then  $\Delta(\underline{x}, \underline{x}') \geq d_2$ , since they may then be considered more properly as elements of  $C_2$ . Similarly for  $\underline{y}$  and  $\underline{y}'$ .

Case 1. Suppose  $\underline{x}$  and  $\underline{x}'$  are in the same coset of  $C_1$ . Then also  $\underline{y}$  and  $\underline{y}'$  are in the same coset of  $C_3$ . If  $\underline{x} = \underline{x}'$ , then  $\Delta(\underline{c}_1, \underline{c}_2) = \Delta(\underline{y}, \underline{y}') \geq d_1$ . If  $\underline{x} \neq \underline{x}'$ , then  $\Delta(\underline{c}_1, \underline{c}_2) = \Delta(\underline{x}, \underline{x}') + \Delta(\underline{y}, \underline{y}') \geq d_1 + d_1 = 2d_1$ .

Case 2. Suppose  $\underline{x}$  and  $\underline{x}'$  are in different cosets of  $C_1$  so that  $\underline{y}$  and  $\underline{y}'$  are also in different cosets of  $C_3$ . Then  $\Delta(\underline{c}_1, \underline{c}_2) = \Delta(\underline{x}, \underline{x}') + \Delta(\underline{y}, \underline{y}') \geq d_2 + d_4$ .

The result follows. QED

Sloane, Reddy and Chen also presented the following three constructions which were originally due to Goethals [5].

Construction Y1. Consider a linear  $(n, d; 2^{k_1})$ -code  $C_1$  and its dual  $(n, d_2; 2^{r_1})$ -code  $C_2$  and translate all the vectors of  $V_n$  so that the codeword of minimum weight in  $C_2$  is  $11\dots 100\dots 0$ . Let  $S$  be the subgroup of  $C_1$  in which the first  $d_2 - 1$  coordinates are zero. Then the  $d_2^{\text{th}}$  coordinates of  $S$  are also zero. By deleting the first  $d_2$  coordinates of codewords in  $S$ , we have a linear  $(n - d_2, d_1; 2^{k_1 - d_2 + 1})$ -code.

Construction Y2. Let  $U$  be the union of  $S$  and all of the  $d_2 - 1$  cosets of  $S$  in  $C_1$  with coset leaders  $110^{n-2}$ ,  $1010^{n-3}$ ,  $10^{d_2-2}10^{n-d_2}$ , where  $0^k$  represents  $k$  consecutive zeros. If we delete the first  $d_2$  coordinates of the vectors of  $U$  we have a nonlinear  $(n - d_2, d_1 - 2; d_2 2^{k_1 - d_2 + 1})$ -code.

Construction Y3. Let  $U$  be the union of  $S$  and all the  $\binom{d_2}{2}$  cosets



of  $S$  in  $C_1$  with coset leaders of weight 2. By deleting the first  $d_2$  coordinates of the vectors of  $U$  we get an  $(n - d_2, d_1 - 4; (1 + \binom{d_2}{2})2^{k_1 - d_2 + 1})$ -code.

Many examples for the preceding constructions as well as encoding and decoding procedures for  $X$  and  $X_4$  may be found in [24].

There are constructions of one code from another that are simpler than those discussed thus far in this section. Elementary constructions can be developed from some of the observations of Section 4 and while many of the results do not appear to be good, they provide the best lower bounds for  $A(n, d)$  that are known for some values of  $n$  and  $d$ . As examples, consider

Construction Q1. Using the method employed in the proof of Proposition 4.3, a lower bound for  $A(n, d)$  can be derived from a lower bound for  $A(n + 1, d)$  by partitioning the codewords of an  $(n + 1, d; A)$ -code  $C$  into two sets, those ending in 0 and those ending in 1. Since there are at least  $\frac{A}{2}$  vectors in one of these sets, there is an  $(n, d; \frac{A}{2})$ -code  $C_1$  so that  $A(n, d) \geq \frac{A}{2}$ .

Construction Q2. Consider the last two coordinates of the codewords of an  $(n, d; A)$ -code  $C$ . Since there are four possibilities for these two positions, the codewords can be partitioned into four sets at least one of which contains at least  $\frac{A}{4}$  vectors. Thus there is an  $(n - 2, d; \frac{A}{4})$ -code  $C_1$  so that  $A(n - 2, d) \geq \frac{A}{4}$ .

Construction Q3. Given an  $(n, d; A)$ -code  $C$ , then we can add a parity check digit to all the codewords of  $C$ , giving an  $(n + 1, d; A)$ -code  $C_1$ . Thus  $A(n + 1, d) \geq A$ .

As an example of construction Q2, the known optimal  $(15,5;256)$ -code of Nordstrom and Robinson demonstrates that  $A(13,5) \geq 64$ . This is the best known lower bound for  $A(13,5)$ , nearly approaching the upper bound of 65 given by Johnson. Similarly, we can use construction Q3 to derive an  $(32,11;2048)$ -code from the known BCH  $(31,11;2048)$ -code.

#### IV. THE PACKING PROBLEM AND REFINED UPPER BOUNDS

##### 13. Johnson's Approach to the Packing Problem

As discussed in Section 5, Hamming developed the sphere packing bound by surrounding each codeword  $\underline{c}$  with a sphere of radius  $e$  and counting those vectors in  $V_n$  at most Hamming distance  $e$  from  $\underline{c}$ ; i.e. all those vectors inside the  $e$ -sphere. Dividing the total number of vectors in  $V_n$  by the number of vectors inside a single sphere, he determined an upper bound for  $A(n, 2e + 1)$ . Johnson [10] has improved the sphere packing bound by considering the set of vectors not contained in any of these spheres and developing lower bound estimates on the cardinality of this set.

As defined in Section 5, codes which satisfy the sphere packing bound are called perfect codes and have the property that every vector in  $V_n$  belongs to exactly one of the  $e$ -spheres about the codewords. For a nonperfect binary  $(n, 2e + 1)$ -code  $C$ , there exists at least one vector of  $V_n$  at distance greater than  $e$  from every codeword; i.e. there is a  $\underline{v}$  in  $V_n$  that belongs to no  $S_e(\underline{c})$  for any  $\underline{c}$  in  $C$ , where  $S_e(\underline{c})$  is as defined at the beginning of Section 5.

Before developing the general Johnson bound, we consider a class of binary codes introduced by Goethals and Snover [6] which they call nearly perfect, that satisfy a specialized version of the Johnson bound. Define  $T(\underline{c})$  to be the set of vectors at distance  $e + 1$  from a specific codeword  $\underline{c}$  and partition  $T(\underline{c})$  into the classes

$$T_\alpha(\underline{c}) = \{\underline{x} \text{ in } T(\underline{c}) : \exists \underline{a} \text{ in } C, \underline{x} \in S_e(\underline{a})\} \text{ and}$$

$$T_\beta(\underline{c}) = \{\underline{x} \in T(\underline{c}) : \underline{x} \notin S_e(\underline{a}), \forall \underline{a} \in C\}.$$

Proposition 13.1. For each  $\underline{c} \in C$ ,  $|T_\alpha(\underline{c})| \leq [(n - e)/(e + 1)] \binom{n}{e}$ .

Proof. If  $\underline{x} \in T_\alpha(\underline{c})$ , then  $\Delta(\underline{x}, \underline{c}) = e + 1$  and  $\underline{x} \in S_e(\underline{a})$  for some  $\underline{a} \in C$  so that  $\Delta(\underline{a}, \underline{x}) \leq e$ . Then  $\Delta(\underline{a}, \underline{x}) + \Delta(\underline{x}, \underline{c}) \leq e + e + 1 = 2e + 1$ . Since  $\underline{a}$  and  $\underline{c}$  are codewords, we have  $2e + 1 \leq \Delta(\underline{a}, \underline{c})$  and by the triangle inequality we have  $2e + 1 \leq \Delta(\underline{a}, \underline{c}) \leq \Delta(\underline{a}, \underline{x}) + \Delta(\underline{x}, \underline{c}) \leq 2e + 1$  which gives  $\Delta(\underline{a}, \underline{c}) = 2e + 1$ . Then  $|T_\alpha(\underline{c}) \cap S_e(\underline{a})| = \binom{2e + 1}{e + 1}$  and so  $|T_\alpha(\underline{c})| = \binom{2e + 1}{e + 1} |N_{2e+1}(\underline{c})|$  where  $N_{2e+1}(\underline{c})$  is the set of codewords at distance  $2e + 1$  from  $\underline{c}$ . Any two vectors in  $N_{2e+1}(\underline{c})$  are at least distance  $2e + 1$  from each other, so the  $(2e + 1)$ -sets of positions in which they both differ from  $\underline{c}$  can have at most  $e$  elements in common. But there are at most  $[(n - e)/(e + 1)]$  of these  $(2e + 1)$ -subsets of an  $n$ -set sharing exactly  $e$  elements, so that

$$|N_{2e+1}(\underline{c})| \leq \frac{[(n - e)/(e + 1)] \binom{n}{e}}{\binom{2e + 1}{e + 1}}$$

and thus  $|T_\alpha(\underline{c})| = \binom{2e + 1}{e + 1} |N_{2e+1}(\underline{c})| \leq [(n - e)/(e + 1)] \binom{n}{e}$ . QED

Proposition 13.2. For each  $\underline{c} \in C$ ,

$$|T_\beta(\underline{c})| \geq \binom{n}{e + 1} - [(n - e)/(e + 1)] \binom{n}{e}.$$

Proof. Since for  $\underline{c} \in C$ ,  $|T_\alpha(\underline{c})| + |T_\beta(\underline{c})| = |T(\underline{c})| = \binom{n}{e + 1}$ , then the result follows from Proposition 13.1. QED

The specialized Johnson bound of Goethals and Snover is presented in

Theorem 13.3. For any code of length  $n$  and minimum distance

$2e + 1$ ,

$$|C| \cdot \left( 1 + \binom{n}{1} + \binom{n}{2} + \dots + \binom{n}{e} + \frac{1}{[n/(e + 1)]} \binom{n}{e} \left( \frac{n - e}{e + 1} - \left[ \frac{n - e}{e + 1} \right] \right) \right) \leq 2^n.$$



Proof. There are at least  $|\bigcup_{\underline{c} \in C} T_\beta(\underline{c})|$  vectors of  $V_n$  that are not contained in any  $e$ -sphere about a codeword of  $C$ . Since codewords are at least distance  $2e + 1$  from each other, a given vector of  $V_n$  can belong to at most  $[n/(e + 1)]$  distinct  $T_\beta(\underline{c})$  for  $\underline{c} \in C$ . By Proposition

$$13.2, |\bigcup_{\underline{c} \in C} T_\beta(\underline{c})| \geq \frac{|C|}{[n/(e + 1)]} ((e + 1)^n - [\frac{n - e}{e + 1}] \binom{n}{e}).$$

But  $2^n \geq \bigcup_{\underline{c} \in C} (S_e(\underline{c}) \cup T_\beta(\underline{c}))$  from which it follows that

$$\begin{aligned} 2^n &\geq |C| [1 + \binom{n}{1} + \dots + \binom{n}{e}] + |C| \left[ \frac{1}{[n/(e + 1)]} ((e + 1)^n - [\frac{n - e}{e + 1}] \binom{n}{e}) \right] \\ &= |C| (1 + \binom{n}{1} + \dots + \binom{n}{e}) + \frac{1}{[n/(e + 1)]} \binom{n}{e} (e + 1)^n - [\frac{n - e}{e + 1}] \binom{n}{e}. \quad \text{QED} \end{aligned}$$

Johnson's own result depends upon the function  $R(m, r, \lambda)$  whose value is the maximum number of vectors of length  $m$  and weight  $r$  such that the inner product of any pair is at most  $\lambda$ ; i.e. they have at most  $\lambda$  ones in common. For example, the vectors (11100) and (00111) show that  $R(5, 3, 1) \geq 2$ . Also important in the development of Johnson's bound is the partitioning of  $V_n$  into disjoint subsets  $S_i$  for  $0 \leq i \leq d - 1$ , where given an  $(n, d)$ -code  $C$ ,

$S_0$  = the set of codewords; i.e. those vectors at least distance  $d$  from each other,

$S_k$  = the subset of vectors at distance  $k$  from at least one of the elements of  $S_0$  and at least distance  $k$  from all of the elements of  $S_0$ .

Thus  $V_n = S_0 \cup S_1 \cup \dots \cup S_{d-1}$ . In terms of these  $S_i$ , while Hamming considered only the sets  $S_0, S_1, \dots, S_e$ , Johnson concentrates on the problem of finding a lower bound on the cardinality of  $S_{e+1}$ .

Using these definitions, we present an example of the specialized

version before proceeding with the development of the general Johnson bound. Consider the case where  $n = 18$  and  $d = 3$  and let  $C$  be an  $(18,3;A)$ -code where  $A = A(18,3)$ ; i.e.  $C$  contains the maximum number of codewords for an  $(18,3)$ -code. Then there are  $A$  vectors in  $S_0$  and  $\binom{18}{1}A = 18A$  vectors in  $S_1$ . We consider the case for  $e + 1$ ; i.e. we look at  $S_2$ . Develop an  $|S_2| \times A$  matrix where the columns are indexed by codewords of  $C$  and the rows are indexed by elements of  $S_2$ . Assign a one to those entries of the matrix whose indexing codeword is at distance two from its indexing element of  $S_2$ , and assign a zero otherwise. If  $N$  is the number of ones in the matrix, bounds for  $N$  may be determined by considering column and row sums of the matrix.

The number of ones in any row is given by the number of codewords at distance  $e + 1$  ( $=2$ ) from a given vector of weight two. By translating this vector of weight two to the origin, the problem is reduced to choosing disjoint pairs of ones from the 18 coordinates; i.e. for each element in  $S_2$  there are at most  $\lfloor \frac{18}{2} \rfloor = 9$  codewords at distance two. Note that the pairs of ones must be disjoint since  $d$  is 3. Thus  $N \leq 9|S_2|$ . Note that  $9|S_2| = \lfloor \frac{n}{e+1} \rfloor |S_e + 1|$ . Next consider the number of ones in each column; i.e. the number of vectors in  $S_2$  that are at distance two from each codeword. If  $\underline{x}$  is any vector of  $V_{18}$ , the number of codewords at least distance 3 from  $\underline{x}$  is at most  $R(18,3,1) = 48$ . Without loss of generality and for simplicity of discussion, translate  $V_n$  so that the vector  $\underline{x}$  is the zero vector. In considering the number of ones in each column, we must subtract those vectors of weight two that are at distance one from codewords of weight three. Since there are at most 48 codewords of weight three,

there are at most  $\binom{3}{1}48 (=144)$  vectors of weight two at distance one from them. But there are  $\binom{18}{2} (= 153)$  vectors at distance two from  $\underline{x}$ , so there are at least  $153 - 144 = 9$  vectors in  $S_2$  and therefore at least nine ones in each column, so that  $N \geq 9A$ . Thus  $9A \leq N \leq 9|S_2|$  which implies  $A \leq |S_2|$ . Since  $V_{18} = S_0 \cup S_1 \cup S_2$ , then  $2^{18} = A + 18A + |S_2| \geq A + 18A + A = 20A$  and finally  $A \leq \frac{2^{18}}{20} = 13107$ , which is the best known upper bound for  $A(18,3)$ .

Returning to the development of the general Johnson bound, consider an  $(n,d)$ -code  $C$  where  $d = 2e + 1$  and let  $\underline{c}$  be any codeword in  $S_0$ . Without loss of generality, translate all vectors in  $V_n$  so that  $\underline{c}$  is the vector of all zeros. Let  $W_k$  denote the resulting set of vectors in  $V_n$  of weight  $k$  and thus distance  $k$  from  $\underline{c}$ . By Proposition 3.7(i),  $W_k$  has  $\binom{n}{k}$  elements. Given  $i$  where  $1 \leq i \leq e$ , there are  $\binom{n}{i}$  vectors at distance  $i$  from any given codeword and for distinct codewords there are distinct such sets of vectors. These are simply those vectors within the  $e$ -spheres, so that consideration of these produces the sphere packing bound. We would like to say that there are  $\binom{n}{e+1}$  vectors of weight  $e + 1$  for each codeword, but some overlap may occur; i.e. some vectors may be at distance  $e + 1$  from more than one codeword. The problem is to determine the degree of overlap.

Before proceeding, note that if  $\underline{v}_i$  and  $\underline{v}_j$  are two vectors of weight  $r_i$  and  $r_j$  respectively, then

$$r_i + r_j = 2\lambda_{ij} + d_{ij} \quad (1)$$

where  $\lambda_{ij}$  is the number of coordinates in which  $\underline{v}_i$  and  $\underline{v}_j$  are the same and  $d_{ij}$  is the number of positions in which they differ. For example, if  $\underline{v}_i = (1001)$  and  $\underline{v}_j = (0011)$ , then (1) gives  $2 + 2 = 2(1) + 2$ .



Given any vector in  $W_k$ , then that vector is in some  $S_i$  for  $i \leq k$ . If  $P_r$  is a codeword of weight  $r$ , then  $P_r$  is in  $W_r \cap S_0$ . Similarly if  $Q_r$  is a noncodeword of weight  $r$ , then  $Q_r$  is in  $W_r \cap S_i$  for  $0 < i \leq r$ . Then by (1) we have  $|W_d \cap S_0| \leq R(n, d, e)$ . Given two vectors in  $W_d$  and  $S_0$ , they are both of weight  $d$  and thus  $d_{ij}$  must be even. Then  $d = 2e + 1$  is odd implies  $d_{ij} \geq d + 1$  and  $2\lambda_{ij} + d + 1 \leq 2d$  or  $\lambda_{ij} \leq e$ ; i.e. the number of coordinates in which they coincide is at most  $e$ .

Each of the codewords  $P_d$  has  $\binom{d}{e}$  vectors  $Q_{e+1}$  in  $W_{e+1} \cap S_e$  which are at distance  $e$  from  $P_d$ . From (1),  $d + e + 1 = 2\lambda_{ij} + e$  so that  $\lambda_{ij} = e + 1$ . Thus each one that occurs in the vector  $Q_{e+1}$  also occurs in the codeword  $P_d$ . By the triangle inequality,  $d = 2e + 1$  insures that these  $Q_{e+1}$  are at distance  $e$  from at most one codeword, thus each codeword provides a distinct set of  $\binom{d}{e}$  vectors in  $W_{e+1} \cap S_e$ .

Since every vector in  $W_{e+1}$  must either be in  $W_{e+1} \cap S_e$  or  $W_{e+1} \cap S_{e+1}$ , then  $|W_{e+1} \cap S_{e+1}| \geq \binom{n}{e+1} - \binom{d}{e}R(n, d, e)$ .

A vector  $Q_{e+1}$  in  $W_{e+1} \cap S_{e+1}$  is at distance  $e + 1$  from at most  $\lfloor \frac{n}{e+1} \rfloor$  codewords. To show this result, simply translate all vectors in  $V_n$  so that  $Q_{e+1}$  is the vector of all zeros and consider the number of vectors of weight  $e + 1$  that are at distance at least  $d + 1$  (since  $d$  is odd). By (1),  $2(e + 1) = 2\lambda_{ij} + 2e + 1$  so that  $\lambda_{ij} = 0$  and  $R(n, e + 1, 0) = \lfloor \frac{n}{e+1} \rfloor$ ; i.e. the number of ways to choose disjoint sets of  $e + 1$  ones from  $n$  positions.

Finally, sum over all codewords in  $S_0$ . The vectors in  $S_1, S_2, \dots, S_e$  are counted just once since, as was noted, they are assigned to distinct codewords, but the vectors in  $S_{e+1}$  are counted as many as  $\lfloor \frac{n}{e+1} \rfloor$  times. Thus divide the lower bound estimate by  $\lfloor \frac{n}{e+1} \rfloor$  so that the result is



$$|C| + |C|\binom{n}{1} + \dots + |C|\binom{n}{e} + |C| \frac{\binom{n}{e+1} - \binom{d}{e}R(n,d,e)}{[n/e + 1]} \leq 2^n.$$

Therefore we have

Theorem 13.4. (Johnson Bound [10]).

$$A(n,d) \leq 2^n \left( 1 + \binom{n}{1} + \binom{n}{2} + \dots + \binom{n}{e} + \frac{\binom{n}{e+1} - \binom{d}{e}R(n,d,e)}{[n/e + 1]} \right)^{-1}$$

From the preceding proposition, it is clear that Johnson's bound is extremely dependent on the values of the function  $R(n,d,e)$ . One bound that he presented was  $R(n,d,e) \leq \left[ \frac{n}{d} \left[ \frac{n-1}{d-1} \left[ \dots \left[ \frac{n-e}{d-e} \right] \right] \right] \right]$  where the value on the right represents nested integral values. Most of the improvements that Johnson has made in [11] were improvements on the bound for  $R(n,d,e)$ . One that was not he found by taking a given  $(n,d)$ -code  $C$  and using parity check constructions to derive two  $(n+1, d+1)$ -codes, one having codewords only of even weight, the other having codewords only of odd weight. By developing independent upper bounds for each code, he derived an improved upper bound on  $A(n,d)$  by taking  $A(n,d) = \min(A_e, A_o)$  where  $A_e(A_o)$  is the upper bound for an  $(n+1, d+1)$ -code of only even (odd) weight.

As a direct result of Theorem 13.4, we have

Proposition 13.5. If  $n$  is even,  $A(n,3) \leq \frac{2^n}{n+2}$ .

Proof. Let  $n = 2m$ . Then by Theorem 13.4,

$$A(n,3) \leq \frac{2^n}{1 + n + \frac{\binom{2m}{2} - \binom{3}{1}R(2m,3,1)}{\left[\frac{2m}{2}\right]}} = 2^n / (1 + n + 1) = 2^n / (n + 2). \text{ QED}$$

Remark. The bound for an  $(18,3)$ -code presented earlier in this section is an example of the result in Proposition 13.5.

For  $d = 5$  and  $n = 2^m - 1$  where  $m$  is an even integer such that  $m \geq 4$ , we have

$$R(2^m - 1, 5, 2) \leq \left[ \frac{2^m - 1}{5} \left[ \frac{2^m - 2}{4} \left[ \frac{2^m - 3}{3} \right] \right] \right]$$

which Preparata [21] reduced to

$$R(2^m - 1, 5, 2) \leq \frac{(2^m - 1)(2^m - 2)(2^m - 4)}{60}.$$

But then by Theorem 13.4,

$$\begin{aligned} A(2^m - 1, 5) &\leq \frac{2^{2^m-1}}{1 + \binom{2^m-1}{1} + \binom{2^m-1}{2} + \left( \binom{2^m-1}{3} - \binom{5}{2} R(2^m - 1, 5, 2) \right)} \\ &\leq \frac{2^{2^m-1}}{1 + \binom{2^m-1}{1} + \binom{2^m-1}{2} + 3 \left( \frac{\frac{(2^m-1)(2^m-2)}{6}}{(2^m-1)} \right)} \\ &= \frac{2^{2^m-1}}{1 + \binom{2^m-1}{1} + \binom{2^m-1}{2} + (2^{m-1} - 1)} \\ &= 2^{2^m-2m}. \end{aligned}$$

This result proves that the Preparata codes presented in Section 9 are optimal.

#### 14. Inequalities Involving Weight Distributions of Codewords

As another approach to the packing problem, an upper bound for the function  $A(n,d)$  can be developed by employing inequalities involving the weight distributions of the codewords. In the case that the minimum distance between codewords is at least three, the method presented in this section provides the sphere packing bound.

Given a code  $C$  of block length  $n$ , let  $W_i$  denote the number of codewords of weight  $i$ , where  $0 \leq i \leq n$ . Clearly  $C = W_0 + W_1 + \dots + W_n$ .

Proposition 14.1. Given an  $(n,3)$ -code  $C$ , then

$$(n - i + 1)W_{i-1} + W_i + (i + 1)W_{i+1} \leq \binom{n}{i}.$$

Proof. Clearly the maximum number of vectors of weight  $i$  is  $\binom{n}{i}$ , the number of ways of choosing  $i$  ones from  $n$  places. If  $\underline{c}$  is any codeword of weight  $i - 1$ , there are  $(n - (i - 1))$  vectors of weight  $i$  adjacent to it, none of which may be codewords as their distance from  $\underline{c}$  is only one. Given two codewords  $\underline{c}_1$  and  $\underline{c}_2$  of weight  $i - 1$ , they must not be adjacent to the same vector  $\underline{v}$  of weight  $i$  since by the triangle inequality this would imply

$\Delta(\underline{c}_1, \underline{c}_2) \leq \Delta(\underline{c}_1, \underline{v}) + \Delta(\underline{c}_2, \underline{v}) = 1 + 1 = 2$ , contradicting that the minimum distance is three. Similarly, there are  $i + 1$  vectors of weight  $i$  adjacent to each codeword of weight  $i + 1$ , none of which are codewords since they are at distance one. Again by the triangle inequality, the sets of vectors of weight  $i$  adjacent to distinct codewords of weight  $i + 1$  are disjoint. There can be no vector of weight  $i$  adjacent to both a codeword of weight  $i - 1$  and one of weight  $i + 1$ , since that would give distance two between these codewords. Finally, since there are  $W_{i-1}$  codewords of weight  $i - 1$  and  $W_{i+1}$  codewords of weight  $i + 1$ , we have

$$(n - i + 1)W_{i-1} + W_i + (i + 1)W_{i+1}. \quad \text{QED}$$

We proceed by example. Let  $C$  be an  $(8,3)$ -code and consider the  $\binom{8}{4} = 70$  vectors of weight four, some of which may be codewords. Thus  $W_4 \leq 70$ , but a closer approximation for  $W_4$  is desirable. Given a codeword of weight five, it is adjacent to five vectors of weight four, none of which are codewords since  $d$  is three. By the triangle inequality, no vector of weight four can be adjacent to two codewords of weight five, and so there are  $5W_5$  vectors of weight four adjacent to the codewords of weight five. Similarly, given a codeword of weight three, there are  $8 - 3 = 5$  vectors of weight four adjacent to it, none of which can be codewords. Again using the triangle inequality, no vector of weight four can be adjacent to two codewords of weight three, so there are  $5W_3$  vectors of weight four adjacent to the codewords of weight three. Thus  $5W_3 + W_4 + 5W_5 \leq 70$ . Continuing these arguments produces the following system of numbered inequalities:

0.	$W_0 + W_1$	$<$	1
1.	$8W_0 + W_1 + 2W_2$	$<$	8
2.	$7W_1 + W_2 + 3W_3$	$<$	28
3.	$6W_2 + W_3 + 4W_4$	$<$	56
4.	$5W_3 + W_4 + 5W_5$	$<$	70
5.	$4W_4 + W_5 + 6W_6$	$<$	56
6.	$3W_5 + W_6 + 7W_7$	$<$	28
7.	$2W_6 + W_7 + 8W_8$	$<$	8
8.	$W_7 + W_8$	$<$	1

Without loss of generality, we can assume the vector of all zeros is a codeword. If not, we may translate all vectors so that one of the codewords becomes the zero vector. Since the minimum distance between codewords is at least three, it necessarily follows that  $W_1 = W_2 = 0$ .



Adding lines 3, 4 and 5 gives (a)  $6W_3 + 9W_4 + 6W_5 + 6W_6 \leq 182$

which implies (b)  $2W_3 + 3W_4 + 2W_5 + 2W_6 \leq \left[\frac{182}{3}\right] = 60$

Adding lines 4 and 5 gives (c)  $5W_3 + 5W_4 + 6W_5 + 6W_6 \leq 126$

Since  $W_1 = W_2 = 0$ ,

line 3 gives (d)  $W_3 \leq \left[\frac{28}{3}\right] = 9$

Adding b, c, and d gives (e)  $8W_3 + 8W_4 + 8W_5 + 8W_6 \leq 194$

which implies (f)  $W_3 + W_4 + W_5 + W_6 \leq \left[\frac{194}{8}\right] = 24$

Adding f to line 8 gives (g)  $W_3 + W_4 + W_5 + W_6 + W_7 + W_8 \leq 25$

Since  $W_0 = 1$  and  $W_1 = W_2 = 0$ , then  $|C| = \sum_{i=0}^8 W_i \leq 26$  and it follows that  $A(8,3) \leq 26$ .

Considering only those inequalities involving  $W_k$  in a general system of inequalities, for any  $k$  we have

$$\begin{aligned} (n-k+2)W_{k-2} + W_{k-1} + kW_k \\ (n-k+1)W_{k-1} + W_k + (k+1)W_{k+1} \\ (n-k)W_k + W_{k+1} + (k+2)W_{k+2} \end{aligned}$$

Adding all  $n+1$  lines in the system, the sum of the left sides of the inequalities is  $(n+1)(W_0 + W_1 + \dots + W_n)$  and the sum of the binomial coefficients on the right is  $2^n$ ; i.e. the inequality resulting from the sum is  $(n+1)|C| \leq 2^n$  or  $|C| \leq 2^n/(n+1)$ . Thus  $A(n,3) \leq 2^n/(n+1)$ , the sphere packing bound for  $d=3$ . In the preceding example, the integral nature of the sum to the left of the inequality allowed replacement of values on the right by the greatest integer in them. For example,  $\frac{182}{3}$  was replaced by  $\left[\frac{182}{3}\right]$ . Such replacements provided an improvement over the sphere packing bound for  $A(8,3)$ , which is 28.4. A further result using this system of inequalities is presented in Section 15.

## 15. An Exemplary Result on Weight Distribution

Many results have been presented using the weight distribution of codewords. In Section 14, such a distribution was used to develop inequalities helpful in determining an upper bound for  $A(n,d)$ . It was also noted that adding the system of inequalities produced the sphere packing bound. For perfect codes, such as the Hamming codes, the sphere packing bound is realized and the inequality derived by totalling the entire system must actually be strict equality, which implies that strict equality must hold for each line of the system. In these cases, the exact weight distribution of the codewords can be determined.

As an example, consider the Hamming  $(15,3;2^{11})$ -code  $C$ . Without loss of generality, assume that the zero vector is a codeword. If it were not, translate all vectors in  $V_{15}$  so that the zero vector becomes a codeword. Let  $W_i$  denote the number of codewords of weight  $i$ . Thus  $|C| = \sum_{i=0}^{15} W_i$ . By Proposition 14.1,

$$(n - (i - 1))W_{i-1} + W_i + (i + 1)W_{i+1} \leq \binom{n}{i}.$$

Since we are concerned with a perfect Hamming code, there must be strict equality in all equations; i.e.  $(n - (i - 1))W_{i-1} + W_i + (i + 1)W_{i+1} = \binom{n}{i}$ . The system of equations is:

$$\begin{array}{rcl}
& X_0 + X_1 & = 1 \\
15X_0 + X_1 + 2X_2 & & = 15 \\
14X_1 + X_2 + 3X_3 & & = 105 \\
13X_2 + X_3 + 4X_4 & & = 455 \\
12X_3 + X_4 + 5X_5 & & = 1365 \\
11X_4 + X_5 + 6X_6 & & = 3003 \\
10X_5 + X_6 + 7X_7 & & = 5005 \\
9X_6 + X_7 + 8X_8 & & = 6435 \\
8X_7 + X_8 + 9X_9 & & = 6435 \\
7X_8 + X_9 + 10X_{10} & & = 5005 \\
6X_9 + X_{10} + 11X_{11} & & = 3003 \\
5X_{10} + X_{11} + 12X_{12} & & = 1365 \\
4X_{11} + X_{12} + 13X_{13} & & = 455 \\
3X_{12} + X_{13} + 14X_{14} & & = 105 \\
2X_{13} + X_{14} + 15X_{15} & & = 15 \\
X_{14} + X_{15} & & = 1
\end{array}$$

Since we assumed that the zero vector is a codeword and the minimum distance between codewords is at least three, we must have  $W_0 = 1$ ,  $W_1 = W_2 = 0$ .

By solving successive equations, the weight distribution is given by

$W_0 = 1$	$W_4 = 105$	$W_8 = 435$	$W_{12} = 35$
$W_1 = 0$	$W_5 = 168$	$W_9 = 280$	$W_{13} = 0$
$W_2 = 0$	$W_6 = 280$	$W_{10} = 168$	$W_{14} = 0$
$W_3 = 35$	$W_7 = 435$	$W_{11} = 105$	$W_{15} = 1$



## 16. A Table of the Best Known Bounds for $A(n,d)$

This section contains a table of the best known upper and lower bounds for  $A(n,d)$  for selected  $n$  and  $d$ . The results are listed in order first by values of  $d$  and then by values of  $n$  for a given  $d$ . We note that extensive tables of upper and lower bounds are presented by Johnson [11] and Sloane [23] respectively.

The columns of Hamming bounds in our table are headed by an H, those of Plotkin by a P, and those of Johnson by a J. We list as Plotkin bounds the best values among those derived from Proposition 4.3, Theorem 5.3 and Corollary 5.4. Those values of the Johnson bound noted by an '\*' are actually Johnson's improvement to Wyner's bound (discussed in [11] and those noted by an '+' are rounded (as they appear in the table given in [11]). Values of the Plotkin and Johnson bounds are often given only for those cases where they provide the best result (i.e. for  $n \leq 2d$  and  $n > 2d$  respectively), while that of Hamming is always listed for comparison.

The reference for the best upper bound is either coded with an H, P or J or with the reference in which it appears. For example,  $A(14,3) \leq 1024$  is due to Johnson (coded J) and  $A(8,3) \leq 20$  is due to Wax (coded [27]). The best lower bound listed in the table is referred to by type of code, which may be identified according to the list below. Also noted in the list (when applicable) are the section(s) of this paper in which the type is discussed and at least one reference in which it appears.

B = BCH code (8;[18,Ch.9])  
H = Hadamard code (10;[15])  
HA = Hamming codes (6,8;[9])  
J = Conference matrix code (10;[25])  
K = Circulant code (6;[14])  
L = Linear code (6;[15],[18,Ch.3],[23])  
N = Nonlinear code (-;[23])  
NRP = Nordstrom-Robinson -Preparata code (9;[17],[20],[21])  
P = Polynomial codes (8;[3],[18,Ch.8])  
QR = Quadratic residue code (8;[18,p.256])  
Q1 = Code from construction Q1 (12;-)  
Q2 = Code from construction Q2 (12;-)  
Q3 = Code from construction Q3 (12;-)  
RM = Reed-Muller code (8;[18,p.125])  
XB = Code from construction X applied to BCH codes (12;[24])  
XC = Code from construction X applied to polynomial codes  
(12;[24])  
XP = Code from construction X applied to Preparata code  
(12;[24])  
X4 = Code from construction X4 (12;[24])  
Y1 = Code from construction Y1 (12;[5])  
Y2 = Code from construction Y2 (12;[5])  
Y3 = Code from construction Y3 (12;[5])  
Z = Code formed by concatenation (11;[16],[26])

$d = 3$ 

	H	P	J	LOWER	REF	UPPER	REF
3	2		--	2	HA	2	H
4	3	2	--	2	HA	2	P
5	5	4	--	4	HA	4	P
6	9	8	--	8	HA	8	P
7	16	16	16	16	P	16	HPJ
8	28	32	25	20	N	20	[27]
9	51	40	51	38	N	39	[27]
10	93	78	81	72	N	78	P
11	170	156	160	144	N	154	[27]
12	315	308	292	256	HA	292	J
13	585	584	585	512	HA	584	P
14	1092	1024	1024	1024	HA	1024	PJ
15	2048	2048	2048	2048	HA	2048	HPJ
16	3855	--	3604	2560	Z	3604	J
17	7281	--	7084	5120	Z	7084	J
18	13797	--	13107	9728	Z	13107	J
19	26214	--	26214	19456	Z	26214	HJ
20	49932	--	47662	36864	Z	47662	J
21	95325	--	95325	73728	Z	95325	H
22	182361	--	173709	147456	Z	173709	J
23	349525	--	344308	294912	Z	344308	J
24	671008	--	645277	$2^{19}$	HA	645277	J
25	1290555	--	1291000	$2^{20}$	HA	1290555	H
26	2485514	--	2397000	$2^{21}$	HA	2397000	J
27	4793492	--	4793000	$2^{22}$	HA	4793000	J
28	9256399	--	8921000	$2^{23}$	HA	8921000	J
29	17895706	--	17730000	$2^{24}$	HA	17730000	J
30	34636850	--	33550000	$2^{25}$	HA	$2^{25}$	H
31	67108896	--	67110000	$2^{26}$	HA	$2^{26}$	H
32	13015024	--	126300000	$5 \cdot 2^{24}$	Z	126300000	J
33	252645248	--	252600000	$5 \cdot 2^{25}$	Z	252600000	J
34	490853619	--	476100000	$5 \cdot 2^{26}$	Z	476100000	J
35	954437581	--	948200000	$5 \cdot 2^{27}$	Z	948200000	J

$d = 5$ 

	H	P	J	LOWER	REF	UPPER	REF
5	2	2	--	2	L	2	HP
6	2	2	--	2	L	2	HP
7	4	3	3	2	L	3	PJ
8	6	4	4	4	L	4	PJ
9	11	6	8	6	H	6	P
10	18	12	13	12	H	12	P
11	30	24	24	24	H	24	PJ
12	51	48	35	32	NRP	35	J
13	89	70	65	64	NRP	65	J
14	154	130	129	128	NRP	129	J
15	270	258	256	256	NRP	256	J
16	478	--	427	256	XP	427	J
17	851	--	851	512	XP	851	HJ
18	1524	--	1424	1024	XP	1424	J
19	2744	--	2427	2048	XP	2427	J
20	4969	--	4741	2560	X4	4741	J
21	9039	--	8651	4096	L	8651	J
22	16513	--	14931	2 <sup>13</sup>	L	14931	J
23	30283	--	29214	2 <sup>14</sup>	L	29214	J
24	55738	--	53382	2 <sup>14</sup>	B	53382	J
25	102927	--	95596	2 <sup>15</sup>	B	95596	J
26	190650	--	190650	2 <sup>16</sup>	B	190650	HJ
27	354136	--	341327	2 <sup>17</sup>	B	341327	J
28	659547	--	616070	2 <sup>18</sup>	B	616070	J
29	1231356	--	1227000	2 <sup>19</sup>	B	1227000	J
30	2304169	--	2226000	2 <sup>20</sup>	B	2226000	J
31	4320896	--	4035000	2 <sup>21</sup>	B	4035000	J
32	8119030	--	7967000	2 <sup>22</sup>	B	7967000	J
33	15284594	--	14850000	2 <sup>22</sup>	NRP	14850000	J
34	28825307	--	27090000	2 <sup>23</sup>	NRP	27090000	J
35	54452876	--	53640000	2 <sup>24</sup>	NRP	53640000	J
36	103027701	--	100100000	2 <sup>25</sup>	NRP	100100000	J
37	195225921	--	185300000	2 <sup>26</sup>	NRP	185300000	J
38	370455643	--	369800000	2 <sup>27</sup>	NRP	369800000	J
39	703912913	--	687000000	2 <sup>28</sup>	NRP	687000000	J
40	1339235024	--	1277000000	2 <sup>29</sup>	NRP	1277000000	J



$d = 7$ 

	H	P	J	LOWER	REF	UPPER	REF
7	2	2	--	2	L	2	HPJ
8	2	2	--	2	L	2	HPJ
9	3	2	--	2	L	2	HPJ
10	5	3	3	2	L	3	PJ
11	8	4	5	4	L	4	P
12	13	5	9	4	RM	5	P
13	21	8	14	8	RM	8	P
14	34	16	22	16	RM	16	P
15	56	32	32	32	RM	32	PJ
16	94	64	54	36	J	54	J
17	157	108	102	64	QR	102	J
18	265	--	167	128	QR	167	J
19	451	--	293	256	QR	293	J
20	776	--	529	512	QR	529	J
21	1342	--	1047	1024	QR	1047	J
22	2337	--	2071	2048	QR	2071	J
23	4096	--	4096	4096	QR	4096	HJ
24	7216	--	6939	4096	Q3	6939	J
25	12777	--	11889	4096	K	11889	J
26	22733	--	20436	$2^{13}$	K	20436	J
27	40622	--	40518	$2^{14}$	K	40518	J
28	72885	--	70002	$2^{14}$	K	70002	J
29	131264	--	121711	$2^{15}$	K	121711	J
30	237238	--	212229	$2^{16}$	K	212229	J
31	430185	--	414950	$2^{16}$	Q3	414950	J
32	782468	--	760242	$2^{17}$	L	760242	J
33	1427375	--	1337000	$19 \cdot 2^{13}$	Z	1337000	J
34	2610925	--	2366000	$9 \cdot 2^{15}$	Z	2366000	J
35	4788148	--	4642000	$9 \cdot 2^{16}$	Z	4642000	J
36	8802294	--	8526000	$2^{20}$	L	8526000	J
37	16218914	--	15430000	$2^{21}$	L	15430000	J
38	29949677	--	27510000	$2^{22}$	L	27510000	J
39	55418954	--	54120000	$2^{23}$	L	54120000	J
40	102748568	--	99860000	$2^{24}$	L	99860000	J
41	190854430	--	181700000	$2^{25}$	L	181700000	J
42	355139638	--	332100000	$2^{26}$	L	332100000	J
43	661958021	--	662000000	$2^{27}$	L	661958021	H
44	1235840934	--	121000000	$2^{28}$	L	121000000	J
45	2310809215	--	221500000	$2^{29}$	L	221500000	J

d = 9

	H	P	J	LOWER	REF	UPPER	REF
9	2	2	--	2	L	2	HPJ
10	2	2	--	2	L	2	HPJ
11	3	2	--	2	L	2	PJ
12	5	2	--	2	L	2	P
13	7	3	--	2	L	3	P
14	11	4	--	4	L	4	P
15	16	5	--	4	Q3	5	P
16	26	6	--	6	H	6	P
17	40	10	--	10	H	10	P
18	64	20	--	20	H	20	P
19	104	40	44	40	H	40	P
20	169	80	70	40	Q3	70	J
21	277	140	135	48	H	135	J
22	460	270	230	52	J	230	J
23	769	--	416	80	Y2	416	J
24	1295	--	757	160	Y2	757	J
25	2196	--	1308	320	Y2	1308	J
26	3748	--	2266	320	Q3	2266	J
27	6436	--	3934	512	B	3934	J
28	11111	--	6774	1024	B	6774	J
29	19283	--	13213	2048	B	13213	J
30	33626	--	23294	3072	Y2	23294	J
31	58904	--	41885	6144	Y2	41885	J
32	103620	--	82275	12288	Y2	82275	J
33	183006	--	161669	24576	Y2	161669	J
34	324417	--	318806	49152	Y2	318806	J
35	577125	--	559732	98304	Y2	559732	J
36	1030092	--	979100	98304	Q3	979100	J
37	1844350	--	1713000	2 <sup>17</sup>	QR	1713000	J
38	3312066	--	3001000	2 <sup>18</sup>	QR	3001000	J
39	5964528	--	5957000	2 <sup>19</sup>	QR	5957000	J
40	10769930	--	10470000	2 <sup>20</sup>	QR	10470000	J
41	19496291	--	18520000	2 <sup>21</sup>	QR	18520000	J
42	35378565	--	32790000	2 <sup>21</sup>	QR	32790000	J
43	64346962	--	58170000	2 <sup>22</sup>	QR	58170000	J
44	117292285	--	11410000	2 <sup>23</sup>	QR	11410000	J
45	214250302	--	210000000	2 <sup>24</sup>	QR	210000000	J

d = 11

	H	P	J	LOWER	REF	UPPER	REF
11	2	2	--	2	L	2	HPJ
12	2	2	--	2	L	2	HJ
13	3	2	--	2	L	2	PJ
14	4	2	--	2	L	2	P
15	6	3	--	2	L	3	P
16	9	3	--	2	L	3	P
17	13	4	--	4	L	4	P
18	20	4	--	4	Q3	4	P
19	31	6	--	4	H	6	P
20	48	8	--	8	B	8	P
21	75	12	--	12	H	12	P
22	118	24	--	24	H	24	P
23	188	48	55	48	H	48	P
24	302	96	91	52	J	91	J
25	490	182	168	64	Q1	168	J
26	801	--	308	128	L	308	J
27	1321	--	585	128	B	585	J
28	2192	--	934	256	B	934	J
29	3662	--	1713	512	B	1713	J
30	6155	--	2793	1024	B	2793	J
31	10406	--	5051	2048	B	5051	J
32	17687	--	9261	2048	Q3	9261	J
33	30217	--	15673	2048	Y1	15673	J
34	51869	--	29068	4096	Y1	29068	J
35	89439	--	48788	8192	Y1	48788	J
36	154876	--	84807	8192	QR	84807	J
37	269268	--	147754	2 <sup>14</sup>	QR	147754	J
38	469929	--	261878	2 <sup>15</sup>	QR	261878	J
39	823076	--	511381	2 <sup>16</sup>	QR	511381	J
40	1446537	--	914100	2 <sup>17</sup>	QR	914100	J
41	2550509	--	1597000	2 <sup>18</sup>	QR	1597000	J
42	4510901	--	2920000	2 <sup>19</sup>	QR	2920000	J
43	8001576	--	5613000	2 <sup>20</sup>	QR	5613000	J
44	14233252	--	10480000	2 <sup>21</sup>	QR	10480000	J
45	25385952	--	20670000	2 <sup>22</sup>	QR	20670000	J

d = 13

	H	P	J	LOWER	REF	UPPER	REF
13	2	2	--	2	L	2	HPJ
14	2	2	--	2	L	2	HPJ
15	3	2	--	2	L	2	PJ
16	4	2	--	2	L	2	P
17	6	2	--	2	L	2	P
18	8	3	--	2	L	3	P
19	11	3	--	2	L	3	P
20	17	4	--	4	L	4	P
21	25	4	--	4	Q3	4	P
22	38	5	--	4	Q3	5	P
23	57	7	--	6	H	7	P
24	88	9	--	8	L	9	P
25	136	14	--	14	H	14	P
26	213	28	--	28	H	28	P
27	337	56	71	56	H	56	P
28	537	112	117	60	J	112	P
29	863	224	202	64	RM	202	J
30	1397	--	385	64	Q3	385	J
31	2278	--	692	72	H	692	J
32	3737	--	1229	76	J	1229	J
33	6171	--	2144	128	XA	2144	J
34	10249	--	3832	256	XA	3832	J
35	17117	--	6244	512	XA	6244	J
36	28734	--	10828	1024	XA	10828	J
37	48475	--	19587	2048	XA	19587	J
38	82160	--	34069	2048	Q3	34069	J
39	139867	--	57463	2048	P	57463	J
40	239103	--	105009	4096	P	105009	J
41	410374	--	193993	8192	P	193993	J
42	706994	--	320073	2 <sup>14</sup>	P	320073	J
43	1222401	--	551600	2 <sup>15</sup>	P	551600	J
44	2120807	--	1017000	2 <sup>15</sup>	Q3	1017000	J
45	3691557	--	1807000	2 <sup>15</sup>	Q3	1807000	J
46	6445784	--	3217000	2 <sup>15</sup>	Y2	3217000	J
47	11288604	--	5708000	2 <sup>16</sup>	Y2	5708000	J
48	19826557	--	9678000	2 <sup>17</sup>	Y2	9678000	J
49	34917638	--	17370000	2 <sup>18</sup>	Y2	17370000	J
50	61657252	--	32370000	2 <sup>19</sup>	Y2	32370000	J



d = 15

	H	P	J	LOWER	REF	UPPER	REF
15	2		--	2	L	2	H
16	2	2	--	2	L	2	HP
17	3	2	--	2	L	2	P
18	4	2	--	2	L	2	P
19	5	2	--	2	L	2	P
20	7	2	--	2	L	2	P
21	10	3	--	2	L	3	P
22	14	3	--	2	L	3	P
23	21	4	--	4	L	4	P
24	31	4	--	4	Q3	4	P
25	46	5	--	4	Q3	5	P
26	69	6	--	6	H	6	P
27	104	8	--	8	L	8	P
28	159	10	--	10	H	10	P
29	246	16	--	16	RM	16	P
30	382	32	--	32	RM	32	P
31	601	64	82	64	RM	64	P
32	951	128	148	64	Q3	128	P
33	1516	256	267	72	H	256	P
34	2434	512	474	76	J	474	J
35	3934	--	851	128	Z	851	J
36	6398	--	1440	128	Z	1440	J
37	10467	--	2674	256	Z	2674	J
38	17216	--	4632	256	XC	4632	J
39	28467	--	8377	512	XC	8377	J
40	47307	--	13723	1024	XC	13723	J
41	78986	--	23839	2048	XC	23839	J
42	132474	--	41934	2048	Q3	41934	J
43	223138	--	74972	2048	L	74972	J
44	377388	--	125866	4096	L	125866	J
45	640756	--	231944	8192	L	231944	J
46	1091975	--	388800	2 <sup>14</sup>	L	388800	J
47	1867567	--	720700	2 <sup>15</sup>	L	720700	J
48	3204919	--	1209000	2 <sup>15</sup>	P	1209000	J
49	5517884	--	2181000	2 <sup>16</sup>	P	2181000	J
50	9529813	--	3812000	2 <sup>17</sup>	P	3812000	J

d = 17

	H	P	J	LOWER	REF	UPPER	REF
17	2	2	--	2	L	2	HP
18	2	2	--	2	L	2	HP
19	3	2	--	2	L	2	P
20	3	2	--	2	L	2	P
21	5	2	--	2	L	2	P
22	6	2	--	2	L	2	P
23	9	3	--	2	L	3	P
24	13	3	--	2	L	3	P
25	18	3	--	2	L	3	P
26	26	4	--	4	L	4	P
27	38	4	--	4	Q3	4	P
28	56	5	--	4	Q3	5	P
29	82	6	--	6	H	6	P
30	124	7	--	6	Q3	7	P
31	187	9	--	8	L	9	P
32	285	12	--	12	H	12	P
33	439	18	--	18	H	18	P
34	681	36	--	36	H	36	P
35	1064	72	99	72	H	72	P
36	1676	144	174	76	J	144	P
37	2656	288	307	80	H	288	P
38	4237	576	554	84	J	554	J
39	6800	1152	944	88	H	944	J
40	10979	--	1808	88	Q3	1808	J
41	17821	--	3017	128	N	3017	J
42	29081	--	4969	128	Q3	4969	J
43	47693	--	8799	128	Q3	8799	J
44	78589	--	16210	256	L	16210	J
45	130089	--	31181	512	L	31181	J
46	216270	--	53013	1024	L	53013	J
47	361035	--	89272	1024	L	89272	J
48	605095	--	148167	2048	L	148167	J
49	1017991	--	256200	4096	L	256200	J
50	1718869	--	448500	4096	Q3	448500	J

d = 19

	H	P	J	LOWER	REF	UPPER	REF
19	2	2	--	2	L	2	HP
20	2	2	--	2	L	2	HP
21	3	2	--	2	L	2	P
22	3	2	--	2	L	2	P
23	4	2	--	2	L	2	P
24	6	2	--	2	L	2	P
25	8	2	--	2	L	2	P
26	11	3	--	2	L	3	P
27	16	3	--	2	L	3	P
28	22	3	--	2	L	3	P
29	32	4	--	4	L	4	P
30	46	4	--	4	Q3	4	P
31	67	5	--	4	Q3	5	P
32	99	5	--	4	Q3	5	P
33	147	6	--	6	H	6	P
34	221	8	--	8	P	8	P
35	333	10	--	10	H	10	P
36	508	13	--	12	H	13	P
37	780	20	--	20	H	20	P
38	1206	40	--	40	H	40	P
39	1877	80	113	80	H	80	P
40	2943	160	204	84	J	160	P
41	4641	320	359	88	H	320	P
42	7365	640	598	88	Q3	598	J
43	11753	1280	1129	96	H	1129	J
44	18859	--	1893	128	L	1893	J
45	30419	--	3197	128	Q3	3197	J
46	49309	--	5918	256	L	5918	J
47	80308	--	10738	512	L	10738	J
48	131390	--	17888	1024	L	17888	J
49	215900	--	29638	1024	Q3	29638	J
50	356245	--	51855	2048	L	51855	J

d = 21

	H	P	J	LOWER	REF	UPPER	REF
21	2	2	--	2	L	2	HP
22	2	2	--	2	L	2	HP
23	2	2	--	2	L	2	HP
24	3	2	--	2	L	2	P
25	4	2	--	2	L	2	P
26	6	2	--	2	L	2	P
27	8	2	--	2	L	2	P
28	10	2	--	2	L	2	P
29	14	3	--	2	L	3	P
30	20	3	--	2	L	3	P
31	28	3	--	2	L	3	P
32	39	4	--	4	L	4	P
33	57	4	--	4	Q3	4	P
34	82	4	--	4	Q3	4	P
35	119	5	--	4	Q3	5	P
36	176	6	--	6	H	6	P
37	262	7	--	6	Q3	7	P
38	392	8	--	8	L	8	P
39	592	11	--	10	H	11	P
40	900	14	--	14	H	14	P
41	1378	22	--	22	H	22	P
42	2126	44	--	44	H	44	P
43	3299	88	132	88	H	88	P
44	5152	176	223	88	Q3	176	P
45	8094	352	391	96	H	352	P
46	12786	704	675	100	J	675	J
47	20306	--	1199	128	P	1199	J
48	32416	--	2041	256	P	2041	J
49	52003	--	3875	256	Q3	3875	J
50	83817	--	6438	256	Q3	6438	J



REFERENCES

1. Berlekamp, E.R., Algebraic Coding Theory, McGraw-Hill, New York, 1968.
2. Bose, R.C., and S.S. Shrikhande, A Note on a Result in the Theory of Code Construction, Inf. and Control 2 (1959), 183-194.
3. Chen, C.L., Computer Results on the Minimum Distance of Some Binary Cyclic Codes, IEEE Trans, PGIT 16 (1970) 359-360.
4. Gilbert, E.N., A Comparison of Signalling Alphabets, Bell System Tech. J. 31 (1952), 504-522.
5. Goethals, J.M., On the Golay Perfect Binary Code, JCT 11 (1971), 178-186.
6. Goethals, J.M., and S.L. Snover, Nearly Perfect Binary Codes, Discrete Math. 3 (1972), 65-88.
7. Golay, M.J.E., Notes on Digital Coding, Proc. IRE 37 (1949), 657.
8. \_\_\_\_\_, Binary Coding, IRE Trans PGIT 4 (1954), 23-28.
9. Hamming, R.W., Error Detecting and Error Correcting Codes, Bell System Tech. J. 29 (1950), 147-160.
10. Johnson, S.M., A New Upper Bound for Error-Correcting Codes, IEEE Trans PGIT 8 (1962), 203-207.
11. \_\_\_\_\_, On Upper Bounds for Unrestricted Binary Error-Correcting Codes, IEEE Trans PGIT 17 (1971), 466-478.
12. Joshi, D.D., Coding Theory, Lecture Notes of Summer Courses for Statisticians No. 4, Indian Statistical Institute, Calcutta, 1963.
13. Julin, D., Two Improved Block Codes, IEEE Trans PGIT 11 (1965), 459.
14. Karlin, M., New Binary Coding Results by Circulants, IEEE Trans PGIT 15 (1969), 81-92.
15. Levenshtein, V.I., Application of the Hadamard Matrix to a Problem of Coding, Problems of Cybernetics 5 (1964), 166-184.
16. Liu, C.L., B.G. Ong and G.R. Ruth, A Construction Scheme for Linear and Nonlinear Codes, Proc. 5th Ann. Princeton Conf. Inform. Sci. (1971), 245-247.
17. Nordstrom, A.W., and J.P. Robinson, An Optimum Nonlinear Code, Inf. and Control 11 (1967), 613-616.
18. Peterson, W.W., and E.J. Weldon, Jr., Error-Correcting Codes, 2nd ed., M.I.T. Press, Cambridge, Mass., 1972.

19. Plotkin, M., Binary Codes with Specified Minimum Distances, IRE Trans PGIT 6 (1960), 445-450.
20. Preparata, F.P., Weight and Distance Structure of Nordstrom-Robinson Quadratic Code, Inf. and Control 12 (1968), 466-473.
21. \_\_\_\_\_, A Class of Optimum Nonlinear Double-Error-Correcting Codes, Inf. and Control 13 (1968), 378-400.
22. Shapiro, H.S., and D.L. Slotnick, On the Mathematical Theory of Error-Correcting Codes, IBM J. Research Develop 3 (1959), 25-34.
23. Sloane, N.J.A., A Survey of Constructive Coding Theory, and a Table of Binary Codes of Highest Known Rate, Discrete Math 3 (1972), 265-294.
24. Sloane, N.J.A., S.M. Reddy and C.L. Chen, New Binary Codes, IEEE Trans PGIT 18 (1972), 503-510.
25. Sloane, N.J.A., and J.J. Seidel, A New Family of Nonlinear Codes Obtained from Conference Matrices, Ann. New York Acad. Sci. 175 (1970), 363-365.
26. Sloane, N.J.A., and D.S. Whitehead, New Family of Single-Error Correcting Codes, IEEE Trans PGIT 16 (1970), 717-719.
27. Wax, N., On Upper Bounds for Error Detecting and Error Correcting Codes of Finite Length, IRE Trans PGIT 5 (1959), 168-174.
28. Bose, R.C., Mathematical Theory of the Symmetrical Factorial Design, Sankhya 8 (1947), 107-166.
29. Bose, R.C., and D.K. Ray-Chaudhuri, On a Class of Error Correcting Binary Group Codes, Inf. and Control 3 (1960), 68-79.
30. \_\_\_\_\_, Further Results on Error Correcting Binary Group Codes, Inf. and Control 3 (1960), 279-290.
31. Mann, H., and D.K. Ray-Chaudhuri, Lectures on Error Correcting Codes, Orientation Lecture Series No. 6, Mathematics Research Center, United States Army, The University of Wisconsin, Madison, Wisconsin.
32. Varsharmov, R.R., Estimate of the Number of Signals in Error Correcting Codes, Doklady Akad. Nauk. SSSR [N.S.] 117 (1957), 739-741.



#### ACKNOWLEDGEMENT

I wish to express my gratitude to Professor Richard Wilson for his assistance and encouragement in the preparation of this paper.

I also wish to thank Professor D. K. Ray-Chaudhuri for his encouragement and support.

This work was supported in part by ONR Contract No. N00014-67-A-0232-0016 (OSURF Project 3430-A1).



# TABLE OF CONTENTS

	Page
ACKNOWLEDGMENTS. . . . .	ii
Chapter	
I. ASSOCIATION SCHEMES. . . . .	1
Introduction	
Two class association schemes	
Association schemes of higher order	
Association matrices	
II. PARAMETERS. . . . .	11
Parameters of two class association schemes	
Sufficient conditions for the existence of a	
three class association scheme	
Triangle numbers	
More useful relationships among parameters	
III. CONSTRUCTING THREE CLASS ASSOCIATION SCHEMES. . . . .	27
Constructing three class association schemes from	
strongly regular graphs	
Constructing three class association schemes	
from rings	
Constructing three class association schemes from	
other combinatorial structures	
Other constructions	
IV. SUMMARY. . . . .	38
APPENDIX. . . . .	39
REFERENCES. . . . .	48

## CHAPTER I

### ASSOCIATION SCHEMES

#### §0. Introduction

The term association scheme was first introduced in 1952 by Bose and Shimamoto [7]. However, the concept of association scheme is inherent in the definition of partially balanced designs which were introduced by Bose and Nair [6] in 1939. Association schemes are very important combinatorial structures, being closely related to projective planes, projective spaces and  $t$  - designs.

Let  $X$  be a set of  $v$  elements and denote by  $P_2(X)$  the complete graph on  $X$ , i.e. the set of  $\frac{1}{2} v(v-1)$  unordered pairs  $\{x, y\}$ ,  $x, y \in X$ ,  $x \neq y$ . Any subset of  $P_2(X)$  will be called a graph on  $X$ . By an  $m$ -class association scheme on  $X$  we mean a partition  $S = \{G_1, G_2, \dots, G_m\}$  of  $P_2(X)$  into  $m$  non-empty graphs  $G_i$  for which:

- (i) there are integers  $n_i$ ,  $1 \leq i \leq m$ , such that for any  $x \in X$ , the number of  $y \in X$  with  $\{x, y\} \in G_i$  is precisely  $n_i$  (each of the  $G_i$  is regular of valence  $n_i$ ),
- (ii) there are integers  $p_{jk}^i$ ,  $1 \leq i, j, k \leq m$  such that for

any  $\{x, y\} \in G_i$  the number of  $z \in X$  with  $\{x, z\} \in G_j$   
and  $\{y, z\} \in G_k$  is precisely  $p_{j k}^i$ .

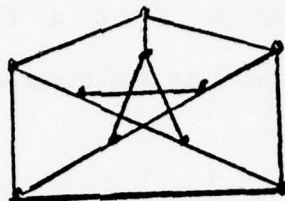
If  $\{x, y\} \in G_i$  we say  $x$  and  $y$  are  $i$ -th associates. The numbers  $v, m, n_i, p_{j k}^i$  are called the parameters of  $S$ .

### §1. Two class association schemes

For the case  $m = 2$  there are eleven parameters,  
 $v, n_1, n_2, p_{11}^1, p_{22}^2, p_{12}^1, p_{22}^1, p_{12}^2, p_{21}^2, p_{11}^2$ . It is clear that the  
scheme is completely determined by  $G_1$  alone. If a pair  
 $\{x, y\} \notin G_1$  then it must be an element of  $G_2$ . Therefore, when  
 $m = 2$  we call  $G_1$  a strongly regular graph with parameters  
 $(n_1, p_{11}^1, p_{11}^2, v)$ . As this definition would imply, the parameters  
of an association scheme are by no means all independent. When  
 $m = 2$ , all parameters can be determined from  $n_1, p_{11}^1, p_{11}^2$ ,  
and  $v$ . The relationships among parameters will be discussed more  
extensively in Chapter 2.

The Petersen graph is a strongly regular graph with parameters  
 $(3, 0, 1, 10)$ . The 2-class association scheme defined by the  
Petersen graph has parameters:

$$\begin{array}{llll} n_1 = 3, & p_{11}^1 = 0, & p_{21}^1 = 2, & p_{21}^2 = 2, \\ n_2 = 6, & p_{22}^2 = 3, & p_{22}^1 = 4, & p_{11}^2 = 1, \\ v = 10, & p_{12}^1 = 2, & p_{12}^2 = 2, & \end{array}$$



The Petersen Graph

The term, strongly regular graph, was introduced by Bose [4] in 1963. However, the strongly regular graph as a structure has been studied extensively for the last twenty years and some deep results are established. Much less is known about association schemes of higher order.

## §2. Association schemes of higher order

Despite the lack of results concerning schemes of higher order, there are some very simple ways to construct examples. The following two constructions show that there exist  $m$ -class association schemes for all positive integers  $m$ .

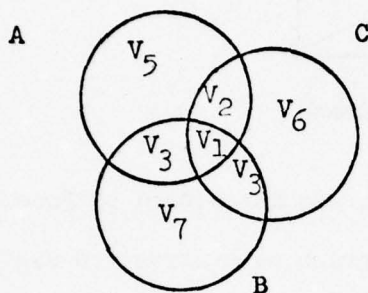
Proposition 1.1 Given a set of  $n$  elements, let  $X$  be the set of all  $m$ -subsets where  $m \leq n$ . If  $G_i$  is the set of unordered pairs  $\{M, N\}$  where  $M, N \in X$  and  $|M \cap N| = m - i$ , then  $S = \{G_1, \dots, G_m\}$  defines an  $m$ -class association scheme.

Proof. Clearly  $S$  is a partition of  $P_2(X)$ .

$n_i = \binom{m}{m-i} \binom{n-m}{i}$ . Calculating  $p_{jk}^i$  requires a little more work. Consider sets  $A$  and  $B$  such that  $|A \cap B| = m - i$ . We



wish to count the number of sets such that  $|A \cap C| = m - j$  and  $|B \cap C| = m - k$ . Let us view  $A \cup B \cup C$  as the union of disjoint sets  $V_1, \dots, V_7$  as illustrated in the diagram below.



Since  $A$  and  $B$  are  $i$ -th associates, we know that

$|V_5 \cup V_2| = |V_7 \cup V_3| = i$  and  $|V_4 \cup V_1| = m - i$ . Let us assume that  $|V_1| = s$ . Then from the conditions on  $C$  we know that

$|V_2 \cup V_1| = m - j$ ,  $|V_1 \cup V_3| = m - k$ ,  $|V_2| = m - j - s$ ,  $|V_3| = m - k - s$ , and  $|V_6| = s + k + j - m$ .

The elements of  $V_1$  must come from  $A \cap B$ . Therefore, there are  $\binom{m-i}{s}$  possible ways to form  $V_1$ . The elements of  $V_2$  must come from  $A \setminus A \cap B$ . Therefore, there are  $\binom{i}{m-j-s}$  possible ways to form  $V_2$ . Similarly there are  $\binom{i}{m-k-s}$  possibilities for  $V_3$ . Finally, the elements of  $V_6$  come from the complement of  $A \cup B$ . Therefore, there are  $\binom{n-m-i}{s+k+j-m}$  possible ways to form  $V_6$ . Clearly then, if  $|V_1| = s$  then there are

$$\binom{m-i}{s} \binom{i}{m-j-s} \binom{i}{m-k-s} \binom{n-m-i}{s+k+j-m}$$

possible ways to form  $C$ . In order to count all possible  $C$  we

must let  $s$  vary from 0 to  $m - i$ . Thus,

$$p_{jk}^i = \sum_{s=0}^{m-i} \binom{m-i}{s} \binom{i}{m-j-s} \binom{n-m-i}{s+k+j-m} \binom{i}{m-k-s}$$

In particular this number is independent of the choice of sets  $A, B$  with  $|A \cap B| = m - i$ .

Proposition 1.2 Given a set of  $n$  elements, let  $X$  be the set of all ordered  $m$ -tuples. If  $G_i$  is the set of unordered pairs  $\{A, B\}$  where  $A, B \in X$  and  $A$  and  $B$  differ in exactly  $i$  coordinates, then  $S = \{G_1, \dots, G_m\}$  defines an  $m$ -class association scheme.

Proof.  $S$  is clearly a partition of  $P_2(X)$ . It can be calculated that  $n_i = (n-1)^i \binom{m}{m-i}$ . To calculate  $p_{jk}^i$  consider  $m$ -tuples  $A$  and  $B$  which are  $i$ -th associates.  $A$  and  $B$  differ in  $i$  coordinates and agree in  $m - i$  coordinates. We wish to count all  $m$ -tuples  $C$  such that  $A$  and  $C$  differ in exactly  $j$  coordinates and  $B$  and  $C$  differ in exactly  $k$  coordinates. Let  $s$  be the number of coordinates in which  $A, B$ , and  $C$  all agree. We can choose these  $s$  coordinates from the  $m - i$  coordinates where  $A$  and  $B$  agree.  $C$  must also agree with  $A$  in  $m - j - s$ , other coordinates. We can choose these from the  $i$  coordinates where  $A$  and  $B$  differ. Similarly,  $C$  must agree with  $B$  in  $m - k - s$  other coordinates to be chosen from the  $i - m + j + s$  remaining coordinates. We need now only consider what choices we have for filling in the coordinates of  $C$  which do not agree with  $A$  and/or  $B$ . What remains of the  $m - i$  coordinates where  $A$

and B agree can be filled with any of  $n - 1$  elements of  $X$ .

What remains of the  $i$  coordinates where A and B differ can be filled with any of  $n - 2$  elements of  $X$ . Therefore,

$$p_{j,k}^i = \sum_s \binom{m-i}{s} \binom{i}{m-j-s} \binom{i-m+j+s}{m-k-s} (n-1)^{a_s} (n-2)^{b_s},$$

where  $a_s = m - i - s$  and  $b_s = i - 2m + 2s + k + j$ .

### §3 Association matrices.

Given an association scheme, we can define relations

$R_0, R_1, \dots, R_m$  on  $X$  as follows:

(i)  $R_0(x, y) = 1$  if  $x = y$ ;  $R_0(x, y) = 0$  otherwise,

(ii)  $R_i(x, y) = 1$  if  $x$  and  $y$  are  $i$ -th associates;

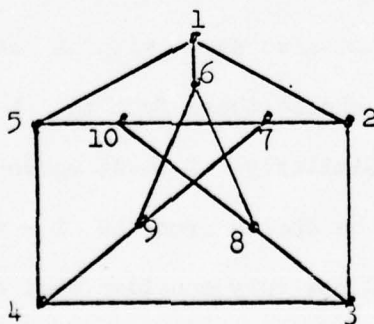
$R_i(x, y) = 0$  otherwise.

If we order the set  $X = \{x_1, \dots, x_v\}$  we can then view the relations as matrices.

$R_i = (r_{\ell, m})$  where  $r_{\ell, m} = R_i(x_\ell, x_m)$ .

Thus defined,  $R_i$  is called an association matrix.

As an example let us order the vertices of the Petersen graph.



Then the association matrices are as follows:

$$R_0 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$R_1 = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \end{pmatrix}$$



$$R_2 = \begin{pmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

The conditions on the association scheme force conditions on the association matrices as the following theorem illustrates. The theorem is due to Bose and Mesner [5].

Theorem 1.3 Let  $S = \{G_1, \dots, G_m\}$  be an  $m$ -class association scheme with parameters  $v, n_1, p_{jk}^i$ , and let  $R_0, R_1, \dots, R_m$  be the association matrices defined above. Then  $R_0 = I, R_1, \dots, R_m$  are nonzero symmetric  $0-1$  matrices of order  $v$  and

$$(i) \quad R_0 + R_1 + \dots + R_m = J,$$

$$(ii) \quad R_j R_k = \sum_i p_{jk}^i R_i.$$

Conversely, if we are given nonzero symmetric  $0-1$  matrices of order  $v$  with conditions (i) and (ii), then they are association matrices of an  $m$ -class association scheme.

Proof. Clearly  $R_i$  are  $0-1$  matrices. Since

$R_i(x_\ell, x_m) = R_i(x_m, x_\ell)$ , the  $R_i$  are also symmetric.

(i) follows from the fact that  $S$  is a partition. For each pair  $\{x_\ell, x_m\}$  there is exactly one  $i$  such that  $\{x_\ell, x_m\} \in G_i$ .

Therefore,  $R_i(x_m, x_\ell) = 1$  for exactly one  $i$ . Consider

$$R_0 + \dots + R_m = A = (A_{ij}).$$

$a_{ij} = R_0(x_i, x_j) + R_1(x_i, x_j) + \dots + R_m(x_i, x_j) = 1$  for any choice of  $i$  and  $j$ .

The proof of (ii) is also not difficult. Consider

$$R_j R_k = A = (a_{\ell m}). \quad \text{Here } a_{\ell m} = \sum_{i=1}^v R_j(x_\ell, x_i) R_k(x_i, x_m).$$

$R_j(x_\ell, x_i) R_k(x_i, x_m) = 1$  if  $x_i$  and  $x_\ell$  are  $j$ -th associates and  $x_i$  and  $x_m$  are  $k$ -th associates;  $R_j(x_\ell, x_i) R_k(x_i, x_m) = 0$  otherwise. Therefore  $a_{\ell m}$  counts the number of  $x \in X$  such that  $x$  is a  $j$ -th associate of  $x_\ell$  and a  $k$ -th associate of  $x_m$ . We know, however, that  $p_{jk}^s$  is the number of  $x \in X$  such that  $x$  is a  $j$ -th associate of  $y$  and  $x$  is a  $k$ -th associate of  $z$  where  $y$  and  $z$  are  $s$ -th associates. We can, therefore, write  $a_{\ell m}$  in terms of  $p_{jk}^i$ 's, namely,  $a_{\ell m} = \sum_s p_{jk}^s R_s(x_\ell, x_m)$ . All the terms in this sum are zero except for the  $s$ -th term where  $x_\ell$  and  $x_m$  are  $s$ -th associates.

For the converse part of the theorem, suppose that we are given nonzero symmetric 0 - 1 matrices  $R_0 = I, R_1, \dots, R_m$  of order  $v$  satisfying (i) and (ii) above. Let  $X = \{x_1, x_2, \dots, x_v\}$  and let  $G_i$  be the set of unordered pairs  $\{x_j, x_k\}$  such that the  $(j, k)$ -entry of  $R_i$  is 1. Then it is easy to check that

$S = \{G_1, \dots, G_m\}$  is an  $m$ -class association scheme on  $X$ , and  $S$  clearly has  $R_0 = I, R_1, \dots, R_m$  as its association matrices.

In working with association schemes, it is often easier to translate conditions on the scheme to conditions on the association matrices and proceed from there.

## CHAPTER II

### PARAMETERS

#### §1. Parameters of 2-class association schemes.

In Chapter 1 we defined a strongly regular graph with parameters  $(n_1, p_{11}, p_{11}^2, v)$  to be  $G_1$  of a 2-class association scheme with parameters  $v, n_i, p_{jk}^i; i, j, k = 1, 2$ . The following proposition proves that strongly regular graphs are well defined.

Given a set  $X$  and a partition  $S = \{G_1, \dots, G_m\}$  of  $P_2(X)$ , we will let  $p_{jk}(x, y)$  denote the number of  $z \in X$  such that  $\{x, z\} \in G_j$  and  $\{y, z\} \in G_k$  for  $x, y \in X$ . In the statement of the next proposition and in the statement of later propositions we will abbreviate the statement, "there exists an integer  $p_{jk}^i$  such that  $p_{jk}(x, y) = p_{jk}^i$  whenever  $x$  and  $y$  are  $i$ -th associates," and simply say " $p_{jk}^i$  exists".

Proposition 2.1 Given a set  $X = \{x_1, \dots, x_l\}$  let  $S = \{G_1, G_2\}$  be a partition of  $P_2(X)$  with  $G_1$  and  $G_2$  regular. Then  $S$  is a 2-class association scheme if  $p_{11}^1$  and  $p_{11}^2$  exist.  
Proof. Let  $A = (a_{ij})$  where  $a_{ij} = 1$  if  $\{x_i, x_j\} \in G_1$  and  $a_{ij} = 0$  otherwise. Let  $B = (b_{ij})$  where  $b_{ij} = 1$  if  $\{x_i, x_j\} \in G_2$  and  $b_{ij} = 0$  otherwise.  $A$  and  $B$  are clearly 0 - 1 matrices. We know  $\{x_i, x_j\} \in G_k$  implies  $\{x_j, x_i\} \in G_k$ , therefore,



$A$  and  $B$  are symmetric. Also, since  $S$  partitions  $P_2(X)$ ,  $A + B + I = J$ . Furthermore, if  $n_1$  is the valence of  $G_1$ , and  $n_2$  is the valence of  $G_2$  then  $AJ = JA = n_1 J$  and  $BJ = JB = n_2 J$ . If the set  $\{aA + bB + cI \mid a, b, c \in R\}$  of all linear combinations of  $A, B, I$  with real coefficients is closed under multiplication, then  $A$  and  $B$  satisfy the conditions of Theorem 1.3 and are, therefore, association matrices of a 2-class association scheme.

We have integers  $p_{11}^1$  and  $p_{11}^2$ , therefore,  
 $A^2 = p_{11}^1 A + p_{11}^2 B + n_1 I$ . But  $A + B + I = J$  implies  
 $A^2 = AJ - AB - AI = n_1 J - AB - A$ . Therefore,  $AB$  is a linear combination of  $A, B$ , and  $I$  and is symmetric. Thus,  $AB = BA$  and  $BA$  is a linear combination of  $A, B$ , and  $I$ . Only  $B^2$  is left. But  $B^2 = BJ - BA - BI = n_2 J - BA - B$ . Therefore,  $B^2$  is a linear combination of  $A, B$ , and  $I$ .

Using the properties of association schemes, it is possible to establish relationships between the parameters.

Proposition 2.2 Let  $S = \{G_1, G_2\}$  be a 2-class association scheme on  $X$ . Then,

- (i)  $n_1 + n_2 + 1 = v$ ,
- (ii)  $p_{12}^1 = p_{21}^1, p_{12}^2 = p_{21}^2$ ,
- (iii)  $p_{12}^1 = n_1 - p_{11}^1 - 1$ ,
- (iv)  $p_{12}^2 = n_1 - p_{11}^2$ ,
- (v)  $p_{22}^1 = v - 2n_1 + p_{11}^1$ ,

$$(vi) \quad p_{22}^2 = v - 2n_1 + p_{11}^2 - 2,$$

$$(vii) \quad n_1 p_{12}^1 = n_2 p_{11}^2, \quad p_{22}^1 = n_2 p_{12}^2,$$

$$(viii) \quad p_{11}^2 (v - n_1 - 1) = n_1 (n_1 - 1 - p_{11}^1).$$

Proof. (i)  $A + B + I = J$  implies  $AJ + BJ + IJ = J^2$ , implies

$$n_1 J + n_2 J + J = vJ, \text{ implies } n_1 + n_2 + 1 = v.$$

$$(ii) \quad AB = BA \text{ implies } p_{12}^1 A + p_{12}^2 B = p_{21}^1 A + p_{21}^2 B,$$

implies  $p_{12}^1 = p_{21}^1$  and  $p_{12}^2 = p_{21}^2$ .

$$(iii) \text{ and } (iv) \quad A^2 = p_{11}^1 A + p_{11}^2 B + n_1 I \text{ and}$$

$$A^2 = AJ - AB - A = (n_1 - p_{12}^1 - 1) A + (n_1 - p_{12}^2) B + n_1 I \text{ imply}$$

$$p_{11}^1 = n_1 - p_{12}^1 - 1 \text{ and } p_{11}^2 = n_1 - p_{12}^2.$$

$$(v) \text{ and } (vi) \quad B^2 = p_{22}^1 A + p_{22}^2 B + n_2 I \text{ and}$$

$$B^2 = n_2 J - AB - B = n_2 A + n_2 B + n_2 I - p_{12}^1 A - p_{12}^2 B - B.$$

$$\text{Therefore, } p_{22}^1 = n_2 - p_{12}^1 = v - 1 - n_1 - (n_1 - p_{11}^1 - 1) =$$

$$v - 2n_1 + p_{11}^1 \text{ and } p_{22}^2 = n_2 - p_{12}^2 - 1 = v - 1 - n_1 - (n_1 - p_{11}^2) - 1 =$$

$$v - 2n_1 + p_{11}^2 - 2.$$

$$(vii) \quad A(AB) = A(p_{12}^1 A + p_{12}^2 B) = p_{12}^1 (p_{11}^1 A + p_{11}^2 B + n_1 I) +$$

$$p_{12}^2 (p_{12}^1 A + p_{12}^2 B). \quad A^2 B = (p_{11}^1 A + p_{11}^2 B + n_1 I) B =$$

$$p_{11}^1 AB + p_{11}^2 B^2 + n_1 B = p_{11}^1 (p_{12}^1 A + p_{12}^2 B) + p_{11}^2 (p_{22}^1 A + p_{22}^2 B$$

$$+ n_2 I) + n_1 B. \text{ Since } A(AB) = (AA)B \text{ we can equate the co-}$$

$$\text{efficients of } I; \quad p_{12}^1 n_1 = p_{11}^2 n_2. \text{ Similarly, since}$$

$$A(BB) = (AB)B, \quad n_1 p_{22}^1 = n_2 p_{12}^2.$$

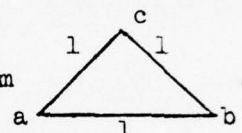
(viii) Since  $n_2 p_{11}^2 = n_1 p_{12}^1$ ,  $p_{11}^2 (v - n_1 - 1) = n_1 (n_1 - 1 - p_{11}^1)$  by (i) and (iii).

From Proposition 2.2 we can conclude that there are at most three independent parameters,  $v, n_1, p_{11}^1$ . In addition, these three parameters must satisfy some easily checked conditions.

Proposition 2.3 If  $S = \{G_1, G_2\}$  is a 2-class association scheme then

- (i)  $G_1$  has  $\frac{1}{6} v n_1 p_{11}^1$  triangles,
- (ii)  $vn_1 \equiv 0 \pmod{2}$ ,
- (iii)  $vn_1 p_{11}^1 \equiv 0 \pmod{3}$ .

Proof. (i) We wish to count triangles of the form



There are  $v$  choices for  $a$ , then  $n_1$  choices for  $b$ , then  $p_{11}^1$  choices for  $c$ . But then, we have counted each set  $\{a, b, c\}$  6 times.

(ii) Since  $G_1$  is regular  $|G_1| = \frac{vn_1}{2}$ .

(iii)  $vn_1 p_{11}^1 \equiv 0 \pmod{3}$  since  $\frac{1}{6} vn_1 p_{11}^1$  is an integer.

In the case of 2-class association schemes, therefore, we have reduced the problem considerably. Given a scheme we need only check 2 parameters  $p_{11}^1$  and  $p_{11}^2$  to be sure it is a 2-class association scheme. Furthermore, in determining possible parameter sets we need only consider choices for  $v, n_1$ , and  $p_{11}^1$ , and these are limited by Proposition 2.3.

§2. Sufficient conditions for the existence of a 3-class association scheme.

The following proposition is analogous to Proposition 2.1.

Proposition 2.4 Given a set  $X = \{x_1, x_2, \dots, x_v\}$  let  $S = \{G_1, G_2, G_3\}$  be a partition of  $P_2(X)$  with  $G_1, G_2$ , and  $G_3$  regular. Then  $S$  is a 3-class association scheme if there exist integers  $p_{11}^1, p_{22}^2, p_{11}^2, p_{11}^3, p_{12}^1, p_{12}^2, p_{12}^3, p_{22}^1, p_{22}^3$ .

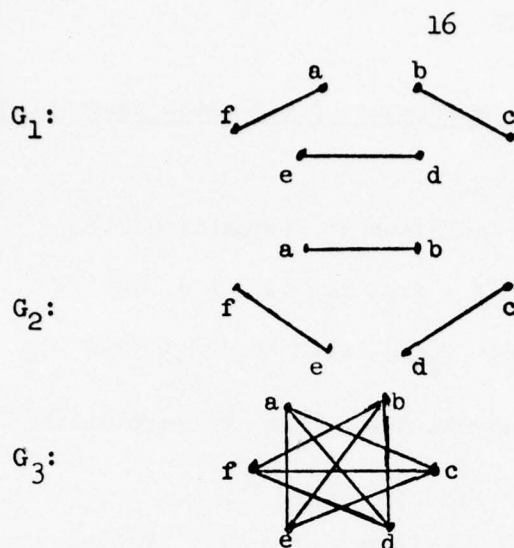
Proof. Define matrices  $A$  and  $B$  in Proposition 2.1. Define  $C = (c_{ij})$  where  $c_{ij} = 1$  if  $\{x_i, x_j\} \in G_3$  and  $c_{ij} = 0$  otherwise. Clearly  $A, B, C$  are 0-1 matrices and are symmetric. Since  $S$  is a partition,  $A + B + C + I = J$ . If the valences of  $G_1, G_2$ , and  $G_3$  are  $n_1, n_2, n_3$  respectively, then  $AJ = JA = n_1 J$ ,  $BJ = JB = n_2 J$ ,  $CJ = JC = n_3 J$ .

If  $\{aA + bB + cC + dI \mid a, b, c, d \in R\}$  is closed under multiplication then  $A, B, C$  satisfy the conditions of Theorem 1.3 and are the association matrices of a 3-class association scheme. We can prove closure by showing that  $A^2, B^2$ , and  $AB$  are linear combinations of  $A, B, C$ , and  $I$ . The rest then follows using  $A + B + C + I = J$ . But, by hypothesis  $A^2 = p_{11}^1 A + p_{11}^2 B + p_{11}^3 C + n_1 I$ ,  $B^2 = p_{22}^1 A + p_{22}^2 B + p_{22}^3 C + n_2 I$ , and  $AB = p_{12}^1 A + p_{12}^2 B + p_{12}^3 C$ .

This result has been observed by Laskar [10].

We can prove that the existence of the 9 parameters is necessary by displaying nonschemes with just one of the 9 missing. For example:



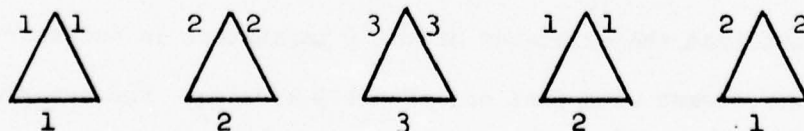


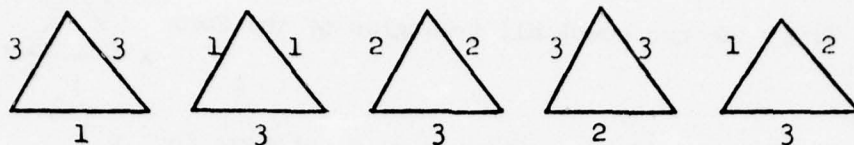
$S = \{G_1, G_2, G_3\}$  is not a 3 class association scheme because  $p_{12}(a,c) = 0$  and  $p_{12}(a,e) = 1$  but  $\{a,c\} \in G_3$  and  $\{a,e\} \in G_3$ .

In other words,  $p_{12}^3$  does not exist. By checking we can determine that  $p_{11}^1, p_{22}^2, p_{11}^2, p_{11}^3, p_{12}^1, p_{12}^2, p_{22}^1$  and  $p_{22}^3$  do exist. Therefore, the existence of  $p_{11}^1, p_{22}^2, p_{11}^2, p_{11}^3, p_{12}^1, p_{22}^1$ , and  $p_{22}^3$  is not sufficient to prove the existence of a 3-class association scheme.

### §3. Triangle numbers.

Given a set  $X$  and any partition  $S$  of  $P_2(X)$ , define a triangle in  $S$  to be an unordered triple  $\{x, y, z\}$  where  $x, y, z$  are distinct elements of  $X$ . If  $S = \{G_1, G_2, G_3\}$  there are ten different kinds of triangles that can occur, with respect to  $S$ .





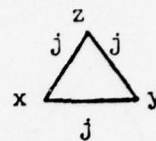
In this geometric representation of a triangle the 3 vertices represent the 3 elements of  $X$  in the triple and the edges represent elements of  $P_2(X)$ . Let  $T_{ijk}$  be the number of triangles of the form  $i \triangle_j k$ . Call  $T_{ijk}$  the  $\{i, j, k\}$  - triangle number.

The order of the  $i, j, k$  is not important.

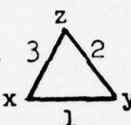
Proposition 2.5 Given a 3-class association scheme on a set  $X$  the following hold:

- (i)  $T_{111} = \frac{1}{6} v n_1 p_{11}^1$
- (ii)  $T_{222} = \frac{1}{6} v n_2 p_{22}^2$
- (iii)  $T_{333} = \frac{1}{6} v n_3 p_{33}^3$
- (iv)  $T_{123} = v n_1 p_{23}^1 = v n_2 p_{13}^2 = v n_3 p_{12}^3$
- (v)  $T_{112} = \frac{1}{2} v n_2 p_{11}^2 = \frac{1}{2} v n_1 p_{12}^1$
- (vi)  $T_{113} = \frac{1}{2} v n_3 p_{11}^3 = \frac{1}{2} v n_1 p_{13}^1$
- (vii)  $T_{221} = \frac{1}{2} v n_1 p_{22}^1 = \frac{1}{2} v n_2 p_{12}^2$
- (viii)  $T_{223} = \frac{1}{2} v n_3 p_{22}^3 = \frac{1}{2} v n_2 p_{23}^2$
- (ix)  $T_{331} = \frac{1}{2} v n_1 p_{33}^1 = \frac{1}{2} v n_3 p_{13}^3$
- (x)  $T_{332} = \frac{1}{2} v n_2 p_{33}^2 = \frac{1}{2} v n_3 p_{23}^3$

Proof. (i) - (iii) We can count all triangles of the form

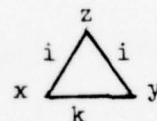


by counting the sets  $\{x, y, z\}$ . There are  $v$  choices for  $x$ ,  $n_j$  choices for  $y$ , and  $p_{jj}^j$  choices for  $z$ . We have, thus, counted each set  $\{x, y, z\}$  6 times.

(iv) Count triangles of the form  in 3 different

ways. There are  $v$  choices for  $x$ ,  $n_1$  choices for  $y$  and  $p_{23}^1$  choices for  $z$ . Therefore  $T_{123} = vn_1 p_{23}^1$ . We can also start with  $y$ . There are  $v$  choices for  $y$ ,  $n_2$  choices for  $z$  and  $p_{13}^2$  choices for  $x$ .  $T_{123} = vn_2 p_{13}^2$ . Thirdly, we can calculate  $T_{123}$  by starting with  $z$ . There are  $v$  choices for  $z$ ,  $n_3$  choices for  $x$ , and  $p_{12}^3$  choices for  $y$ .  $T_{123} = vn_3 p_{12}^3$ .

(v) - (x). We can count triangles of the form



in 2 different ways. There are  $v$  choices for  $x$ ,  $n_k$  choices for  $y$  and  $p_{ii}^k$  choices for  $z$ . Since  $x$  and  $y$  are interchangeable we have counted each triangle twice.  $T_{iik} = \frac{1}{2} vn_k p_{ii}^k$ . We can also start with  $y$ . There are  $v$  choices for  $y$ ,  $n_i$  choices for  $z$ , and  $p_{ik}^i$  choices for  $x$ .  $T_{iik} = \frac{1}{2} vn_i p_{ik}^i$ .

Define an  $\{i, j\}$  - angle to be a pair  $(\{x, y\}, z)$  where  $x, y, z \in X$ ,  $x$  and  $z$  are  $i$ -th associates, and  $y$  and  $z$  are  $j$ -th associates. Let  $A_{ij}$  be the number of  $\{i, j\}$  - angles in a

scheme. Note that  $A_{ij} = A_{ji}$ .

Proposition 2.6 Given a set  $X = \{x_1, \dots, x_v\}$  and a partition  $S = \{G_1, G_2, G_3\}$  of  $P_2(X)$  such that  $G_1, G_2$ , and  $G_3$  are regular of degrees  $n_1, n_2, n_3$  respectively, then:

- (i)  $T_{111} + T_{222} + T_{333} + T_{112} + T_{113} + T_{221} + T_{223} + T_{331} + T_{332} + T_{123} = \binom{v}{3},$
- (ii)  $3T_{111} + T_{112} + T_{113} = \frac{1}{2} v n_1 (n_1 - 1),$
- (iii)  $3T_{222} + T_{221} + T_{223} = \frac{1}{2} v n_2 (n_2 - 1),$
- (iv)  $3T_{333} + T_{331} + T_{332} = \frac{1}{2} v n_3 (n_3 - 1),$
- (v)  $2T_{112} + 2T_{221} + T_{123} = v n_1 n_2,$
- (vi)  $2T_{113} + 2T_{331} + T_{123} = v n_1 n_3,$
- (vii)  $2T_{223} + 2T_{332} + T_{123} = v n_2 n_3.$

Proof. (i) This follows since  $S$  is a partition of a complete graph.

(ii) We can find  $A_{11}$  in 2 ways. Counting  $(\{x, y\}, z)$  there are  $v$  ways to choose  $x, n_1$  ways to choose  $z$  and  $(n_1 - 1)$  ways to choose  $y$ . We have counted each pair twice so  $A_{11} = \frac{1}{2} v n_1 (n_1 - 1)$ .

Also  $x$  and  $y$  can be 1-st associates, 2-nd associates or

3-rd associates. Therefore,  $A_{11} = 3T_{111} + T_{112} + T_{113}.$

(iii) Find  $A_{22}$  in 2 different ways.

(iv) Find  $A_{33}$  in 2 different ways.

(v) - (viii) We can count  $A_{ij}$  in 2 different ways. Count  $(\{x, y\}, z)$ . There are  $v$  choices for  $x, n_i$  choices for  $z$ , and



$n_j$  choices for  $y$ .  $A_{ij} = v n_i n_j$ . Also  $\{i, j\}$  angles appear twice in  $\{i, i, j\}$  - triangles and once in  $\{i, j, k\}$  triangles. Therefore,  
 $A_{ij} = 2T_{iij} + 2T_{ijj} + T_{ijk}$ .

§4. More useful relationships among parameters.

Proposition 2.7 Given a 3-class association scheme, then

$$(i) \quad p_{11}^1 p_{22}^1 + p_{12}^1 p_{22}^2 + p_{13}^1 p_{22}^3 = p_{12}^1 (p_{12}^1 - 1) \\ + p_{22}^1 (p_{12}^2 - 1) + p_{23}^1 (p_{12}^3 - 1),$$

$$(ii) \quad p_{11}^1 p_{23}^1 + p_{12}^1 p_{23}^2 + p_{13}^1 p_{23}^3 = p_{13}^1 p_{12}^1 + p_{23}^1 p_{12}^2 \\ + p_{33}^1 p_{12}^3.$$

Proof. (i) Fix  $x, y \in X$  such that  $R_1(x, y) = 1$ . Count all pairs  $(a, b)$  such that  $R_1(a, x) = 1$ ,  $R_2(a, b) = 1$  and  $R_2(b, y) = 1$ .

Geometrically, we have a rectangle  $\begin{array}{ccc} & 2 & \\ a & \square & b \\ 1 & & 2 \\ x & 1 & y \end{array}$ . We can count the

pairs  $(a, b)$  in 2 different ways. First,  $R_1(x, b) = 1$  or  $R_2(x, b) = 1$  or  $R_3(x, b) = 1$ . Thus we get  $p_{12}^1 (p_{12}^1 - 1) + p_{22}^1 (p_{12}^2 - 1) + p_{32}^1 (p_{12}^3 - 1)$ . Similarly  $R_1(a, y) = 1$  or  $R_2(a, y) = 1$  or  $R_3(a, y) = 1$ . In this way we get  $p_{11}^1 p_{22}^1 + p_{12}^1 p_{22}^2 + p_{13}^1 p_{22}^3$ .

(ii) Fix  $x, y \in X$  such that  $R_1(x, y) = 1$ . Now count the pairs  $(a, b)$  such that  $R_1(a, x) = 1$ ,  $R_2(a, b) = 1$ , and

$R_3(b, y) = 1$ . Geometrically, we have a rectangle  $\begin{array}{ccc} & 2 & \\ a & \square & b \\ 1 & & 3 \\ x & 1 & y \end{array}$ .

Counting the number of rectangles in 2 different ways we establish the equality.

Equations (i) and (ii) of Proposition 2.7 are two cases of a more general family of relations that hold for parameters of m-class schemes. These were noticed by [5] and we give a proof using the association matrices.

Theorem 2.8 Let  $S = \{G_1, \dots, G_m\}$  be an m-class association scheme with association matrices  $R_0, R_1, \dots, R_m$ . Then for  $0 \leq i, j, k, t \leq m$

$$\sum_s p_{jk}^s p_{si}^t = \sum_s p_{ij}^s p_{sk}^t.$$

Proof. We know  $R_i (R_j R_k) = (R_i R_j) R_k$ . Then using (ii) from Theorem 1.3 we get

$$R_i \sum_s p_{jk}^s R_s = \left( \sum_s p_{ij}^s R_s \right) R_k,$$

$$\sum_s p_{jk}^s R_s R_i = \sum_s p_{ij}^s R_s R_k,$$

$$\sum_s p_{jk}^s \sum_t p_{si}^t R_t = \sum_s p_{ij}^s \sum_t p_{sk}^t R_t,$$

$$\sum_{s,t} p_{jk}^s p_{si}^t R_t = \sum_{s,t} p_{ij}^s p_{sk}^t R_t.$$

Therefore,  $\sum_s p_{jk}^s p_{si}^t = \sum_s p_{ij}^s p_{sk}^t$ .

If we write the equalities of Proposition 2.7 in terms of triangle numbers we get:

$$(i) \quad 12n_2 n_3 T_{111} T_{221} + 12n_1 n_3 T_{112} T_{222} + 4n_1 n_2 T_{113} T_{223} = \\ 4n_2 n_3 T_{112}^2 + 4n_1 n_3 T_{221}^2 - n_1 n_2 n_3 v(vn_1 n_2) + n_1 n_2 T_{123},$$

$$\begin{aligned}
 & (ii) \quad 6n_2 n_3 T_{111} T_{123} + 4n_1 n_3 T_{112} T_{223} + 4n_1 n_2 T_{113} T_{332} \\
 & = 4n_2 n_3 T_{113} T_{112} + 2n_1 n_3 T_{123} T_{221} + 2n_1 n_2 T_{331} T_{123} .
 \end{aligned}$$

Of the 10 triangle numbers we can get 6 of them dependent on  $T_{111}, T_{222}, T_{333}, T_{112}$  using Proposition 2.5. In terms of the  $p_{jk}^i$  this means  $p_{11}^1, p_{22}^2, p_{33}^3$ , and  $p_{11}^2$  determine all others. Furthermore, using Proposition 2.7 we can get  $p_{11}^2$  as a quadratic in terms of  $p_{11}^1, p_{22}^2$ , and  $p_{33}^3$ . Thus, given  $p_{11}^1, p_{22}^2$ , and  $p_{33}^3$ , there are only 2 possibilities for  $p_{11}^2$ .

The following is a list of parameters expressed in terms of  $n_1, n_2, n_3, p_{11}^1, p_{22}^2, p_{33}^3$ , and  $p_{11}^2$ .

1.  $p_{12}^1 = \frac{n_2}{n_1} p_{11}^2$
2.  $p_{12}^2 = \frac{1}{3n_2} (n_3^2 - n_3 n_2 - n_1 n_3 - n_3 - n_3 p_{33}^3 + n_2^2 - n_2 p_{22}^2 - n_2 + n_1^2 - n_1 - n_1 p_{11}^1 + 2n_1 n_2) - p_{11}^2$
3.  $p_{22}^1 = \frac{1}{3n_1} (n_3^2 - n_3 n_2 - n_1 n_3 - n_3 p_{33}^3 + n_2^2 - n_2 p_{22}^2 - n_2 + n_1^2 - n_1 - n_1 p_{11}^1 + 2n_1 n_2 - 3n_2 p_{11}^2)$
4.  $p_{22}^3 = \frac{1}{3n_2} (-n_3^2 + n_3 n_2 + n_1 n_3 + n_3 + n_3 p_{33}^3 - n_2^2 + n_2 - n_1^2 + n_1 + n_1 p_{11}^1 - 2n_1 n_2 + 3n_2 p_{11}^2 - 2n_2 p_{22}^2 + 3n_2^2 - 3n_2)$
5.  $p_{11}^3 = \frac{1}{n_3} (n_1^2 - n_1 - n_2 p_{11}^2 - n_1 p_{11}^1)$
6.  $p_{33}^2 = n_3 - n_2 - n_1 + 1 + p_{22}^2 - p_{11}^2 + \frac{2}{3n_2} (n_3^2 - n_3 n_2 - n_3 - n_1 n_3 - n_3 p_{33}^3 + n_2^2 - n_2 p_{22}^2 - n_2 + n_1^2 - n_1 - n_1 p_{11}^1 + 2n_1 n_2)$

$$7. \quad p_{33}^1 = n_3 - n_2 - n_1 + 1 + p_{11}^1 + \frac{1}{3n_1} (3n_2 p_{11}^2 + n_3^2 - n_3 n_2 - n_1 n_3 \\ - n^3 - n^3 p_{33}^3 + n_2^2 - n_2 p_{22}^2 - n_2 + n_1^2 - n_1 p_{11}^1 + 2n_1 n_2) ,$$

$$8. \quad p_{13}^1 = n_1 - 1 - p_{11}^1 - \frac{n_2}{n_1} p_{11}^2 ,$$

$$9. \quad p_{23}^1 = n_2 - \frac{1}{3n_1} (n_3^2 - n_3 n_2 - n_1 n_3 - n_3 - n_3 p_{33}^3 + n_2^2 \\ - n_2 p_{22}^2 - n_2 + n_1^2 - n_1 - n_1 p_{11}^1 + 2n_1 n_2) ,$$

$$10. \quad p_{13}^2 = n_1 - \frac{1}{3n_2} (n_3^2 - n_3 n_2 - n_1 n_3 - n_3 - n_3 p_{33}^3 + n_2^2 \\ - n_2 p_{22}^2 - n_2 - n_1^2 - n_1 - n_1 p_{11}^1 + 2n_1 n_2) ,$$

$$11. \quad p_{12}^3 = \frac{1}{3n_3} (n_1 n_2 - n_3^2 + n_3 n_2 + n_1 n_3 + n_3 + n_3 p_{33}^3 - n_2^2 \\ + n_2 p_{22}^2 + n_2 - n_1^2 + n_1 p_{11}^1 + n_1) ,$$

$$12. \quad p_{23}^2 = n_2 - 1 - p_{22}^2 + p_{11}^2 - \frac{1}{3n_2} (n_3^2 - n_3 n_2 - n_1 n_3 - n_3 \\ - n_3 p_{33}^3 + n_2^2 - n_2 p_{22}^2 - n_2 + n_1^2 - n_1 - n_1 p_{11}^1 + 2n_1 n_2) ,$$

$$13. \quad p_{13}^3 = n_1 - \frac{1}{3n_3} (n_1 n_2 - n_3^2 + n_3 n_2 + n_1 n_3 + n_3 p_{33}^3 - n_2^2 \\ + n_2 p_{22}^2 + n_2 + 2n_1^2 + n_3 - 2n_1 - 3n_2 p_{11}^2 - 2n_1 p_{11}^1) ,$$

$$14. \quad p_{23}^3 = n_2 - \frac{1}{3n_3} ( - 2n_3^2 + 2n_3 n_2 + 2n_1 n_3 + 2n_3 + 2n_3 p_{33}^3 \\ + n_2^2 - n_2 - 2n_1^2 + 2n_1 + 2n_1 p_{11}^1 - n_1 n_2 + 3n_2 p_{11}^2 \\ - n_2 p_{22}^2) .$$

Suppose, for example,  $n_1 = 10$ ,  $n_2 = 10$ ,  $n_3 = 21$ ,  $p_{11}^1 = 3$ ,

$p_{22}^2 = 5$ ,  $p_{33}^3 = 0$ . Then,



$$p_{12}^1 = p_{11}^2$$

$$p_{12}^2 = 10 - p_{11}^2$$

$$p_{22}^1 = 10 - p_{11}^2$$

$$p_{22}^3 = -\frac{20}{7} + \frac{10}{21} p_{11}^2$$

$$p_{11}^3 = \frac{20}{7} - \frac{10}{21} p_{11}^2$$

$$p_{33}^2 = 27 - p_{11}^2$$

$$p_{33}^1 = 14 + p_{11}^2$$

$$p_{13}^1 = 6 - p_{11}^2$$

$$p_{23}^1 = 0$$

$$p_{13}^2 = 0$$

$$p_{13}^3 = \frac{50}{7} + \frac{10}{21} p_{11}^2$$

$$p_{23}^3 = \frac{90}{7} - \frac{10}{21} p_{11}^2$$

$$p_{12}^3 = 0$$

$$p_{23}^2 = -6 + p_{11}^2$$

Using equality (i) of Proposition 2.7 we get

$$\frac{52}{21} (p_{11}^2)^2 - \frac{194}{7} p_{11}^2 + \frac{540}{7} = 0 . \quad p_{11}^2 = 6 \text{ is the only integral root.}$$

In this case, given  $n_1, n_2, n_3, p_{11}^1, p_{22}^2, p_{33}^3$  there is only one possibility for  $p_{11}^2$ . It would seem, however, that the quadratic in  $p_{11}^2$  could have 2 integral roots. To avoid this situation we could choose a different set of independent parameters.

Using previously obtained relationships we can express all  $p_{jk}^i$  in terms of  $n_1, n_2, n_3, p_{11}^1, p_{22}^1, p_{11}^2, p_{22}^2$  as follows:

$$1. \quad p_{12}^1 = \frac{n_2}{n_1} p_{11}^2 ,$$

$$2. \quad p_{12}^2 = \frac{n_1}{n_2} p_{22}^1 ,$$

$$3. \quad p_{22}^3 = \frac{1}{n_3} (n_2^2 - n_1 p_{22}^1 - n_2 p_{22}^2 - n_2) ,$$

$$4. \quad p_{12}^3 = \frac{1}{n_3} (n_1 n_2 - n_2 p_{11}^2 - n_1 p_{22}^1) ,$$

5.  $p_{11}^3 = \frac{1}{n_3} (n_1^2 - n_1 - n_2 p_{11}^2 - n_1 p_{11}^1) ,$
6.  $p_{33}^3 = n_3 - n_2 - n_1 - 1 + \frac{1}{n_3} (n_2^2 - n_1 p_{22}^1 - n_2 p_{22}^2 - n_2$   
 $- n_1^2 - n_1 - n_2 p_{11}^2 - n_1 p_{11}^1)$   
 $+ \frac{2}{n_3} (n_1 n_2 - n_2 p_{11}^2 - n_1 p_{22}^1) ,$
7.  $p_{33}^2 = n_3 - n_2 - n_1 + 1 + p_{22}^2 + 2\frac{n_1}{n_2} p_{22}^1 + p_{11}^2 ,$
8.  $p_{33}^1 = n_3 - n_2 - n_1 + 1 + p_{22}^1 + 2\frac{n_2}{n_1} p_{11}^2 + p_{11}^1 ,$
9.  $p_{32}^3 = n_2 - \frac{1}{n_3} (n_2^2 - 2n_1 p_{22}^1 - n_2 p_{22}^2 - n_2 + n_1 n_2 - n_2 p_{11}^2) ,$
10.  $p_{32}^2 = n_2 - 1 - p_{22}^2 - \frac{n_1}{n_2} p_{22}^1 ,$
11.  $p_{32}^1 = n_2 - p_{22}^1 - \frac{n_2}{n_1} p_{11}^2 ,$
12.  $p_{31}^3 = n_1 - \frac{1}{n_3} (n_1 n_2 - 2n_2 p_{11}^2 - n_1 p_{22}^1 + n_1^2 - n_1 - n_1 p_{11}^1) ,$
13.  $p_{31}^2 = n_1 - \frac{n_1}{n_2} p_{22}^1 - p_{11}^2 ,$
14.  $p_{31}^1 = n_1 - 1 - \frac{n_2}{n_1} p_{11}^2 - p_{11}^1 .$

Then using (i) of Proposition 2.7, we can obtain an equation for  $p_{11}^1$  in terms of  $n_1, n_2, n_3, p_{22}^1, p_{11}^2, p_{22}^2$ . Namely,  $p_{11}^1 = \frac{A}{B}$

where

$$A = -2\frac{n_2 n_1}{n_3} p_{11}^2 - 2\frac{n_1^2}{n_3} p_{22}^1 + \frac{n_1^2}{n_3 n_2} (p_{22}^1)^2$$

$$+ \frac{n_2}{n_3} (p_{11}^2)^2 + \frac{n_1}{n_3} p_{22}^1 p_{11}^2 + \frac{n_1 n_2}{n_3} + \frac{(n_2)^2}{n_3} p_{11}^2$$

$$\begin{aligned}
& + \frac{(n_1)^2}{n_3} - \frac{n_1}{n_3} - \frac{n_2}{n_3} p_{11}^2 + \frac{(n_1)^2}{n_3} p_{22}^2 - \frac{n_1}{n_3} p_{22}^2 \\
& - p_{11}^2 p_{22}^2 - n_1 + \frac{n_2}{n_1} (p_{11}^2)^2 + \frac{(n_1)^2}{(n_2)^2} (p_{22}^1)^2 \\
& - \frac{n_2}{n_3} p_{11}^2 p_{22}^2 + \frac{(n_1)^3}{n_2 n_3} p_{22}^1 - \frac{(n_1)^2}{n_2 n_3} p_{22}^1 \quad \text{and} \\
B &= \frac{n_1}{n_2} p_{22}^1 - \frac{n_1 n_2}{n_3} + \frac{n_1}{n_3} + \frac{n_1}{n_3} p_{22}^2 + \frac{(n_1)^2}{n_2 n_3} p_{22}^1 .
\end{aligned}$$

If  $B \neq 0$  then we can find  $p_{11}^1$  given  $n_1, n_2, n_3, p_{22}^1, p_{11}^2$ , and  $p_{22}^2$ . For example, suppose  $n_1 = 3, n_2 = 3, n_3 = 1$ ,  $p_{22}^2 = 0, p_{11}^2 = 0$ , and  $p_{22}^1 = 2$ . Then  $A = 4$  and  $B = 2$  so  $p_{11}^1 = 2$ . However, suppose  $n_1 = 2, n_2 = 2, n_3 = 2, p_{22}^2 = 0, p_{11}^2 = 1$ , and  $p_{22}^1 = 0$ . Then  $A = 0$  and  $B = 0$  and we cannot determine  $p_{11}^1$  using the above equation.

The parameter problem, therefore, can be reduced. From 3 n's and 27  $p_{jk}^i$ 's we can get down to at most 3 n's and 3 independent  $p_{jk}^i$ 's. The problem is still, however, much more complex than in the case of 2-class association schemes.

## CHAPTER III

### CONSTRUCTING 3-CLASS ASSOCIATION SCHEMES

#### §1. Constructing 3-class association schemes from strongly regular graphs.

Proposition 3.1 Let  $A_1, \dots, A_m$  be  $m$  strongly regular graphs defined on points  $X_1, \dots, X_m$  respectively and with the same parameters  $(n_1, p_{11}^1, p_{11}^2, v)$ . Then we can define a 3-class association scheme on a set  $X$  as follows:

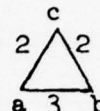
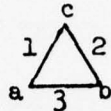
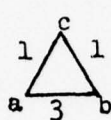
- (i)  $X = X_1 \cup X_2 \cup \dots \cup X_m$ ,
- (ii)  $R_i(x, y) = 1$  for  $x, y \in X$  if and only if  $\{x, y\} \in A_i$   
for some  $i=1, \dots, m$ ,
- (iii)  $R_2(x, y) = 1$  for  $x, y \in X$  if and only if  $x, y \in X_i$  for  
some  $i=1, \dots, m$  and  $\{x, y\} \notin A_i$ ,
- (iv)  $R_3(x, y) = 1$  for  $x, y \in X$  if and only if  $x \in X_i$  and  
 $y \in X_j$  for  $i \neq j$ .

Proof. We can explicitly display the 12 necessary parameters of the 3-class association scheme in terms of the parameters of the strongly regular graphs. By theorem 2.4 we need only show that we have a partition of  $P_2(x)$  into regular graphs and  $p_{11}^1, p_{22}^2, p_{11}^2, p_{11}^3, p_{12}^1, p_{12}^2, p_{12}^3$  exist.  $p_{22}^1$  and  $p_{22}^3$  exist.

Let - distinguish the parameters of the 3-class association



scheme. Clearly  $\bar{p}_{jk}^i = p_{jk}^i$  for  $i, j, k = 1, 2$ . Also  $\bar{n}_i = n_i$  for  $i = 1, 2$ . In addition, it is not difficult to see that the following triangles do not appear:



If  $\{a, c\} \in A_i$  and  $\{b, c\} \in A_i$ , then clearly  $a, b, c \in X_i$ . Similarly, if  $\{a, c\} \in A_i$  and  $b \in X_i$  then  $R_3(a, b) \neq 1$ . Lastly, if  $a, c \in X_i$  and  $c, b \in X_j$  then  $i = j$  and  $a, b, c \in X_i$ . Thus  $R_3(a, b) \neq 1$ .

Because the 3 triangles above do not exist  $\bar{p}_{11}^3 = \bar{p}_{12}^3 = \bar{p}_{22}^3 = 0$ . Since  $\bar{v} = mv$  and  $\bar{n}_3 = (m-1)v$  we have calculated all necessary parameters.

Proposition 3.2 Given a 3-class association scheme on a set  $X$  such that  $T_{113} = T_{123} = T_{223} = 0$  then the scheme can be constructed from strongly regular graphs by the method of Proposition 3.1. Proof. Define a relation  $M$  on  $X$ .  $M(x, y) = 1$  if and only if  $R_3(x, y) = 0$ . Then  $M$  is an equivalence relation  $M(x, x) = 1$ ,  $M(x, y) = M(y, x)$ , and if  $M(x, y) = 1$  and  $M(y, z) = 1$  then  $M(x, z) = 1$ . Otherwise, we would have  $T_{ij3} \neq 0$  for  $i \neq 3$  and  $j \neq 3$ .

Therefore,  $M$  partitions  $X$  into equivalence classes say  $X_1, \dots, X_m$  and  $|X_i| = n_1 + n_2 + 1$ . Also,  $\{z \mid R_1(x, z) = 1\} \subseteq X_i$  for all  $x \in X_i$  and  $\{z \mid R_2(x, z) = 1\} \subseteq X_i$  for all  $x \in X_i$ . Therefore, we can form strongly regular graphs  $A_1, \dots, A_m$  on sets  $X_1, \dots, X_m$  respectively.

Proposition 3.3 Let  $S = \{G_1, G_2\}$  be a 2-class association scheme on  $X$ . We can construct a 3-class association scheme  $S = \{\bar{G}_1, \bar{G}_2, \bar{G}_3\}$  on a set  $\bar{X}$  as follows:

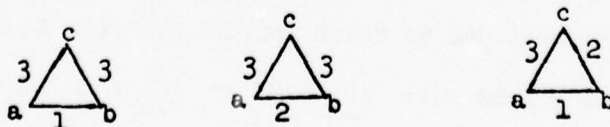
- (i) replace every  $x \in X$  by a set of  $m$  elements  $\{x_1, \dots, x_m\}$  for some fixed  $m$  to form  $\bar{X}$ ,
- (ii) if  $\{x, y\} \in G_1$  then  $\{x_i, y_j\} \in \bar{G}_1$  for all  $i, j=1, \dots, m$ ,
- (iii) if  $\{x, y\} \in G_2$  then  $\{x_i, y_j\} \in \bar{G}_2$  for all  $i, j=1, \dots, m$ ,
- (iv)  $\bar{G}_3$  is the union of complete graphs on each set  $\{x_1, \dots, x_m\}$ .

Proof. By Proposition 2.4 we need only show that we have a partition of  $P_2(x)$  into regular graphs and integers  $p_{11}^1, p_{22}^2, p_{11}^2, p_{11}^3, p_{12}^1, p_{12}^2, p_{12}^3, p_{22}^1, p_{22}^3$  exist.

Let  $\bar{\cdot}$  denote the parameters of the 3-class association scheme. Clearly,  $\bar{v} = mv$ ,  $\bar{n}_1 = mn_1$ , and  $\bar{n}_2 = mn_2$ . Similarly,  $\bar{p}_{jk}^i = m p_{jk}^i$  for  $i, j, k = 1, 2$ .

To calculate  $\bar{p}_{12}^3, \bar{p}_{11}^3$ , and  $\bar{p}_{22}^3$  consider  $a, b \in \bar{X}$  such that  $\{a, b\} \in \bar{G}_3$ . This implies that  $a$  and  $b$  come from the same  $x \in X$  in the 2-class scheme. Therefore,  $\bar{p}_{12}^3 = 0$ ,  $\bar{p}_{11}^3 = mn_1$ , and  $\bar{p}_{22}^3 = mn_2$ . Finally, since  $\bar{G}_3$  is the union of complete graphs on  $m$  elements,  $\bar{n}_3 = m-1$ .

It is interesting to note that the following 3 types of triangles do not occur in these schemes.



Since  $\{a,c\} \in \bar{G}_3$  and  $\{b,c\} \in \bar{G}_3$   $a,b,c$  must come from the same  $x \in X$  and therefore,  $\{a,b\} \in \bar{G}_3$ . We have already shown that  $p_{12}^3 = 0$ .

Proposition 3.4 Given a 3-class association scheme  $S = \{G_1, G_2, G_3\}$  on a set  $X$  with  $T_{133} = T_{233} = T_{123} = 0$ , then the scheme can be constructed from a two-class scheme by the construction of Proposition 3.3.

Proof. Define a relation  $M$  on  $X$ .  $M(x,y) = 1$  if and only if  $R_3(x,y) = 1$  or  $x = y$ . Then  $M$  is an equivalence relation.  $M(x,x) = 1$ ,  $M(x,y) = M(y,x)$ , and if  $M(x,y) = 1$  and  $M(y,z) = 1$  then  $M(x,z) = 1$ . Otherwise,  $T_{i33} \neq 0$  for some  $i \neq 3$ .

Therefore,  $M$  partitions  $X$  into equivalence classes of order  $n_3+1$ . If  $M(x,x') = 1$  then  $\{z | R_i(x,z) = 1\} = \{z | R_i(x',z) = 1\}$  for all  $i$ . Clearly, it is true for  $i = 3$  by definition of  $M$ . For  $i = 2$ , if it is not true there exists a  $z \in X$  such that  $R_2(x,z) = 1$  and  $R_2(x',z) \neq 1$ . Therefore,  $R_1(x',z) = 1$  and  $T_{123} \neq 0$ . Similarly, for  $i = 1$ .

Therefore, we can replace each equivalence class by one element  $\bar{x}$  and the associations will still be well defined.

Since a great deal is known about 2-class schemes these two constructions are helpful in constructing 3-class schemes. We shall, however, eliminate from further discussions some schemes which appear to be of little interest due to their trivial nature. Given a 2-class association scheme with  $p_{11}^2 = 0$  or  $p_{22}^1 = 0$  we shall call it trivial.

If  $p_{11}^2 = 0$  then  $G_1$  is a union of complete graphs and is not connected. If  $p_{22}^1 = 0$  then  $G_2$  is a union of complete graphs. We will classify all 3-class association schemes constructed from trivial 2-class association schemes by the methods of Proposition 3.1 or 3.3 as trivial 3-class association schemes.

It may be worthwhile to note that all trivial 3-class association schemes can be obtained using a construction written up by Blackwelder [3] .

Proposition 3.5 Given  $m = N_1 N_2 N_3$  where  $N_1, N_2, N_3 \geq 2$  let  $X = \{(i_1 i_2 i_3) \mid i_j \in (0, 1, \dots, N_j - 1) \text{ for } j = 1, 2, 3\}$ . Define  $G_j = \{\{x, y\} \mid x, y \in X \text{ and } x \text{ and } y \text{ agree in the first } 3-j \text{ coordinates and disagree in coordinate } 4-j\}$ . Then  $S = \{G_1, G_2, G_3\}$  is a 3-class association scheme.

Proof.  $S$  is clearly a partition of  $P_2(X)$  and we can calculate  $n_1 = N_3 - 1$ ,  $n_2 = N_3(N_2 - 1)$ ,  $n_3 = N_3 N_2(N_1 - 1)$ .

Similarly, we can calculate the necessary 9 parameters as follows:

$$\begin{array}{ll} p_{11}^1 = N_3 - 2, & p_{12}^1 = 0, \\ p_{22}^2 = N_3(N_2 - 2), & p_{12}^2 = N_3 - 1, \\ p_{11}^2 = 0, & p_{12}^3 = 0, \\ p_{11}^3 = 0, & p_{22}^1 = N_3(N_2 - 1). \\ p_{22}^3 = 0, & \end{array}$$



Clearly  $T_{113} = T_{123} = T_{223} = 0$ . Therefore, the schemes are constructed from 2-class schemes by Proposition 3.2. The 2-class schemes are trivial since  $p_{11}^2 = 0$ . Switching 1 and 3,  $T_{113} = T_{112} = T_{123} = 0$ . Therefore, these schemes are also constructed from 2-class schemes by Proposition 3.4. Since  $p_{22}^3 = 0, p_{22}^1 = 0$  in the 2-class scheme and it is therefore trivial.

## §2. Constructing 3-class association schemes from rings.

Proposition 3.6 Let  $R$  be a ring and  $U \subseteq R^*$  such that  $U$  is a group under multiplication and  $-1 \in U$ . Then if  $n$  is the number of associate classes of  $U$  under multiplication, we can define an  $n-1$  class association scheme as follows:

- (i) Let  $S_0, S_1, \dots, S_{n-1}$  be the associate classes of  $U$  where  $S_0 = \{0\}$  and the others are subscripted arbitrarily,
- (ii) let the elements of  $R = X$ ,
- (iii)  $R_i(x, y) = 1$  if and only if  $x - y \in S_i$ .

Proof. Choose  $r_0, \dots, r_{n-1} \in R$  such that  $S_i = r_i U$ . Note that  $x - y \in S_i$  implies  $y - x \in S_i$  since  $-1 \in U$ .

We wish to show that  $p_{ij}^s$  is a constant. Choose  $x$  and  $y$  such that  $x - y \in r_s U$ . Then  $p_{ij}^s$  counts the number of  $z \in R$  such that  $z - x \in r_i U$  and  $z - y \in r_j U$ . Therefore,  $z - x = r_i u_1$  and  $z - y = r_j u_2$  for some  $u_1$  and  $u_2 \in U$ . Also,  $x - y = r_s u_3$  where  $u_3 \in U$ . Then  $z = r_i u_1 + x = r_j u_2 + y$  implies  $r_i u_1 + r_s u_3 = r_j u_2$  (1). Therefore,  $p_{ij}^s$  is the number of ordered pairs  $(u_1, u_2)$  which satisfy equation (1).

Suppose  $R_s(x', y') = 1$  where  $x' - y' = r_s \beta_3$  and  $\beta_3 \neq u_3$ . Then  $p_{ij}^s$  is the number of ordered pairs  $(\beta_1, \beta_2)$  such that  $r_i \beta_1 + r_s \beta_3 = r_j \beta_2$  (2).

To show  $p_{ij}^s$  is a constant we must show that the number of solutions for (1) is the same as the number of solutions for (2). Since  $u_3$  and  $\beta_3 \in U$  there exists  $u_3^{-1}$  and  $\beta_3^{-1} \in U$ . Therefore for each solution  $(u_1, u_2)$  of (1),  $(u_1 u_3^{-1} \beta_3, u_2 u_3^{-1} \beta_3)$  is a solution of (2).

Similarly, if  $(\beta_1, \beta_2)$  is a solution of (2) then  $(\beta_1 \beta_3^{-1} u_3, \beta_2 \beta_3^{-1} u_3)$  is a solution of (1).

Therefore,  $p_{ij}^s$  is a constant.

### §3 Constructing 3-class association schemes from other combinatorial structures.

An orthogonal array  $(N, m, s, t)$  of strength  $t$  is an  $m \times N$  rectangular array in  $N$  assemblies, with  $m$  constraints, in  $s$  symbols, such that in any  $t$ -rowed submatrix of the array each of the  $s^t$  possible column vectors appears exactly  $\lambda$  times where  $\lambda s^t = N$ .  $\lambda$  is called the index of the array.

Proposition 3.7 Suppose we have an  $(n^2, \beta_1 + \beta_2, n, 2)$  orthogonal array where  $n, \beta_1, \beta_2$  are positive integers such that  $n \geq 2$  and  $\beta_1 + \beta_2 \leq n$ . Then let  $X$  be the  $n^2$  assemblies. Define a partition on  $P_2(X)$  as follows:

- (1)  $\{x, y\} \in G$ , if the columns corresponding to  $x$  and  $y$  are alike in exactly one position in the first  $\beta_1$  rows,

- (ii)  $\{x,y\} \in G_2$  if the columns corresponding to  $x$  and  $y$  are alike in exactly one position in the last  $\beta_2$  rows,  
 (iii)  $\{x,y\} \in G_3$  otherwise.

Then  $S = \{G_1, G_2, G_3\}$  is a 3-class association scheme.

Proof. Since the array has strength 2 and index 1, two columns are alike in at most one position. Therefore,  $S$  is a partition.

We can determine explicitly that  $n_1 = \beta_1(n-1)$ ,  $n_2 = \beta_2(n-1)$ ,  $n_3 = \beta_3(n-1)$  where  $\beta_3 = n + 1 - (\beta_1 + \beta_2)$ .

Similarly we can determine the necessary 9 parameters.

$$p_{11}^1 = n - 2 + (\beta_1 - 1)(\beta_1 - 2),$$

$$p_{22}^2 = n - 2 + (\beta_2 - 1)(\beta_2 - 2),$$

$$p_{11}^2 = \beta_1(\beta_1 - 1),$$

$$p_{11}^3 = \beta_1(\beta_1 - 1),$$

$$p_{12}^1 = \beta_2(\beta_1 - 1),$$

$$p_{12}^2 = \beta_1(\beta_1 - 1),$$

$$p_{11}^3 = \beta_1\beta_2,$$

$$p_{22}^1 = \beta_2(\beta_2 - 1),$$

$$p_{22}^3 = \beta_2(\beta_2 - 1).$$

This construction was written up by Blackwelder [3].

An incidence structure is a triple  $(P, B, J)$  where  $P$  and  $B$  are disjoint sets and  $J \subseteq P \times B$ . Elements  $p \in P$  are called points and elements  $b \in B$  are called blocks. A point  $p$  and a block  $b$  are incident iff  $(p, b) \in J$ . For any block  $b$ ,  $\underline{(b)}$  denotes the set of points incident with  $b$ . An  $(n, k, \lambda)$ -symmetric balanced incomplete block design (sbi bd) is an incidence structure  $D = (P, B, J)$  such that

- (i)  $|P| = |B| = n$ ,
- (ii)  $b \in B$  implies  $|(b)| = K$ ,
- (iii)  $T \subseteq P$ ,  $|T| = 2$  implies there exists exactly  $\lambda$  blocks  $b \in B$  with  $T \subseteq (b)$ .

We will need two results in regard to  $(n,k,\lambda)$  - sbibd's . These may be found in [9]. First, if  $p \in P$  then  $p$  is incident with exactly  $k$  blocks. Secondly, given blocks  $b, b' \in B$ ,  $|(b) \cap (b')| = \lambda$ . With these two results we can prove the following proposition.

Proposition 3.8 Given a  $(n,k,\lambda)$  - s b i b d .  $D = (P,B,J)$  we can construct a 3-class association scheme  $S = \{G_1, G_2, G_3\}$  on  $X$  as follows:

- (i)  $X = P \cup B$ ,
- (ii)  $\{v,w\} \in G_1$  for  $v, w \in X$  if  $w, v \in P$  or  $w, v \in B$ ,
- (iii)  $\{v,w\} \in G_2$  for  $v,w \in X$  if  $v \in P, w \in B$  and  $v \in (w)$  or  $w \in P, v \in B$  and  $w \in (v)$ ,
- (iv)  $\{v,w\} \in G_3$  for  $v, w \in X$ , otherwise.

Proof. Clearly  $S = \{G_1, G_2, G_3\}$  is a partition of  $P_2(X)$ . We can easily calculate  $v = 2n$ ,  $n_1 = n - 1$ ,  $n_2 = k$ , and  $n_3 = n - k$

We can also calculate the 9 necessary parameters.

$$\begin{array}{lll}
 p_{11}^1 = n - 2, & p_{22}^2 = 0, & p_{11}^2 = 0, \\
 p_{11}^3 = 0, & p_{12}^1 = 0, & p_{12}^2 = k - 1, \\
 p_{12}^3 = k, & p_{22}^1 = \lambda, & p_{22}^3 = 0.
 \end{array}$$

All  $(n,k,\lambda)$  - s b i b d's on  $n \leq 25$  points have been determined



(see [9]) . They have parameters  $(7,3,1)$  ,  $(11,5,2)$  ,  $(13,4,1)$  ,  $(16,6,2)$  ,  $(15,7,3)$  ,  $(19,9,4)$  ,  $(23,11,5)$  ,  $(21,5,1)$  and  $(25,9,3)$  .

#### §4. Other constructions

The rest of the constructions can be found in an article by Blackwelder [3] .

Proposition 3.9 Given  $n \geq 6$  let  $X = \{(x_1, x_2, x_3) | x_1 \neq x_2 \neq x_3, \text{ unordered triples, } x_1, x_2, x_3 \text{ range from } 0 \text{ to } n-1\}$  . Define  $G_i = \{(x, y) | x, y \in X \text{ and } x \text{ and } y \text{ differ in exactly } i \text{ coordinates}\}$  . Then ,  $S = \{G_1, G_2, G_3\}$  is a 3-class association scheme.

Proof.  $S$  is clearly a partition of  $P_2(X)$  . We can calculate that  $n_1 = 3(n-3)$  ,  $n_2 = \frac{3(n-3)(n-4)}{2}$  , and  $n_3 = \frac{(n-3)(n-4)(n-5)}{6}$  .

We can also calculate the necessary 9 parameters as follows:

$$\begin{aligned} p_{11}^1 &= n-2, & p_{22}^1 &= (n-4)^2, & p_{12}^3 &= 9, \\ p_{22}^2 &= \frac{(n-5)(n+2)}{2}, & p_{12}^1 &= 2(n-4), & p_{22}^3 &= 9(n-6), \\ p_{11}^2 &= 4, & p_{12}^2 &= 2(n-4), & p_{11}^3 &= 0. \end{aligned}$$

Proposition 3.10 Given  $n \geq 2$ , let  $X = \{(x_1, x_2, x_3) | \text{ the triple is ordered and } x_1, x_2, x_3 \text{ range from } 0 \text{ to } n-1\}$  . Define  $G_i = \{(x, y) | x, y \in X \text{ and } x \text{ and } y \text{ differ in exactly } i \text{ coordinates}\}$  . Then  $S = \{G_1, G_2, G_3\}$  is a 3-class association scheme.

Proof. Clearly  $S$  is a partition of  $P_2(X)$  . We can calculate that  $n_1 = 3(n-1)$  ,  $n_2 = 3(n-1)^2$  ,  $n_3 = (n-1)^3$  .

We can also calculate the 9 necessary parameters.

$$\begin{aligned} p_{11}^1 &= n-2, & p_{22}^1 &= 2(n-1)(n-2), & p_{12}^3 &= 3, \\ p_{22}^2 &= n^2-2n+2, & p_{12}^1 &= 2(n-1), & p_{22}^3 &= 6(n-2), \end{aligned}$$

$$p_{11}^2 = 2, \quad p_{12}^2 = 2(n-2), \quad p_{11}^3 = 0.$$

Proposition 3.11 Given  $v = l \cdot n$  where  $l, n \geq 2$ , let  $X$  be any set of  $v$  elements. Arrange the elements of  $X$  in  $l$  rows and  $n$  columns. Define  $G_1 = \{\{x, y\} | x, y \in X \text{ and } x \text{ and } y \text{ are in the same row}\}$ ,  $G_2 = \{\{x, y\} | x, y \in X, \text{ and } x \text{ and } y \text{ are in the same column}\}$ , and  $G_3 = \{\{x, y\} | x, y \in X \text{ and } x \text{ and } y \text{ are not in the same row or same column}\}$ . Then  $S = \{G_1, G_2, G_3\}$  is a 3-class association scheme.

Proof. Clearly  $S$  is a partition of  $P_2(X)$ . We can calculate  $n_1 = n-1$ ,  $n_2 = l-1$ , and  $n_3 = (l-1)(n-1)$ .

We can also calculate the necessary 9 parameters as follows:

$$\begin{array}{lll} p_{11}^1 = n-2, & p_{22}^1 = 0, & p_{12}^3 = 1, \\ p_{22}^2 = l-2, & p_{12}^1 = 0, & p_{22}^3 = 0, \\ p_{11}^2 = 0, & p_{12}^2 = 0, & p_{11}^3 = 0. \end{array}$$

## CHAPTER IV

### SUMMARY

My original intention in this study was to determine all 3-class association schemes on a small number of vertices. This problem has been attacked for strongly regular graphs with fairly complete results being obtained [2]. However, in the case of 3-class association schemes I was unable to resolve the problem of parameters. Where in 2-class association schemes there were 2 parameters, I could at best reduce to no less than 6 parameters. The number of possible parameter sets is thus much too large to attempt to computationally reduce.

I have, however, made a start on the problem. Besides reducing from 30 to 6 or 7 parameters we know that some easily checked relations must hold.  $vn_1 p_{11}^1 = vn_2 p_{22}^2 = vn_3 p_{33}^3 \equiv 0(6)$ .  
 $vn_1 = vn_2 = vn_3 \equiv 0(2)$ .

In addition, I have collected all known constructions which give schemes on less than 50 vertices. In the tables that follow I will display sufficient parameter sets to characterize these schemes, namely  $v, n_1, n_2, n_3, p_{11}^1, p_{22}^2, p_{33}^3, p_{11}^2$ . As a description of one example for each set I have given the proposition number of the construction along with necessary parameters. I have not included in the table schemes constructed from Proposition 3.5 as these I considered of a trivial nature.

No.	v	$n_1$	$n_2$	$n_3$	$p_{11}^1$	$p_{22}^2$	$p_{33}^3$	$p_{11}^2$	Description
1	4	1	1	1	0	0	0	0	$G_1 \equiv G_2 \parallel G_3 \times$
2	6	2	2	1	0	1	0	1	Proposition 3.6 where $R = \mathbb{Z}_6$
3	7	2	2	2	0	0	0	1	Proposition 3.6 where $R = \mathbb{Z}_7$
4	8	2	1	4	0	0	0	2	Proposition 3.6 where $R = \mathbb{Z}_8$
5	8	3	3	1	2	0	0	0	Proposition 3.10 where $n = 2$
6	9	2	2	4	1	1	1	0	Proposition 3.11 where $n = 3, l = 3$
7	10	4	4	1	0	3	0	3	Proposition 3.6 where $R = \mathbb{Z}_{10}$
8	10	2	2	5	0	0	0	1	Proposition 3.1 where $m = 2$ , from $(2,0,1,5)$
9	10	4	4	1	0	0	0	2	Proposition 3.3 where $m = 2$ , from $(2,0,1,5)$
10	12	3	2	6	2	1	2	0	Proposition 3.11 where $n = 4, l = 3$
11	12	5	1	5	4	1	0	0	Proposition 3.11 where $n = 6, l = 2$
12	13	4	4	4	0	0	0	1	Proposition 3.6 where $R = \mathbb{Z}_{13}$
13	14	3	6	4	0	5	0	1	Proposition 3.8 from $(7,3,1)$
14	14	6	6	1	0	5	0	5	Proposition 3.6 where $R = \mathbb{Z}_{14}$



No.	v	$n_1$	$n_2$	$n_3$	$p_{11}^1$	$p_{22}^2$	$p_{33}^3$	$p_{11}^2$	Description
15	15	8	4	2	3	3	1	6	Proposition 3.6 where $R = Z_{15}$
16	15	2	2	10	0	0	5	1	Proposition 3.1 where $m = 3$ , from $(2,0,1,5)$
17	15	6	6	2	0	0	1	3	Proposition 3.3 where $m = 3$ , from $(2,0,1,5)$
18	16	5	5	5	0	0	0	2	Proposition 3.6 where $R = GF(16)$
19	16	3	3	9	2	2	4	0	Proposition 3.11 where $n = 4$ , $l = 4$
20	16	7	1	7	6	0	0	0	Proposition 3.11 where $n = 8$ , $l = 2$
21	16	3	6	6	2	2	2	0	Proposition 3.7 where $\beta_1 = 1$ , $\beta_2 = 2$
22	18	5	2	10	4	1	4	0	Proposition 3.11 where $n = 6$ , $l = 3$
23	18	8	1	8	7	0	0	0	Proposition 3.11 where $n = 9$ , $l = 2$
24	18	4	4	9	1	1	0	2	Proposition 3.1 where $m = 2$ , from $(4,1,2,9)$
25	18	8	8	1	2	2	0	4	Proposition 3.3 where $m = 2$ , from $(4,1,2,9)$
26	19	6	6	6	2	2	2	1	Proposition 3.6 where $R = Z_{19}$
27	20	9	9	1	4	4	0	4	Proposition 3.9 where $n = 6$
28	20	9	1	9	8	0	0	0	Proposition 3.11 where $n = 10$ , $l = 2$
29	20	4	3	12	3	2	6	0	Proposition 3.11 where $n = 5$ , $l = 4$

No.	v	$n_1$	$n_2$	$n_3$	$p_{11}^1$	$p_{22}^2$	$p_{33}^3$	$f_{11}^2$	Description
30	20	3	6	10	0	3	0	1	Proposition 3.1 where $m = 2$ , from $(3,0,1,10)$
31	20	6	12	1	0	6	0	2	Proposition 3.3 where $m = 2$ , from $(3,0,1,10)$
32	20	2	2	15	0	0	10	1	Proposition 3.1 where $m = 4$ , from $(2,0,1,5)$
33	20	8	8	3	0	0	2	4	Proposition 3.3 where $m = 4$ , from $(2,0,1,5)$
34	21	12	6	2	5	5	1	10	Proposition 3.6 where $R = Z_{21}$
35	22	10	10	1	0	9	0	9	Proposition 3.6 where $R = Z_{22}$
36	22	10	5	6	9	0	0	0	Proposition 3.8 from $(11,5,2)$
37	24	11	1	11	10	0	0	0	Proposition 3.11 where $n = 12$ , $l = 2$
38	24	7	2	14	6	1	6	0	Proposition 3.11 where $n = 8$ , $l = 3$
39	24	5	3	15	4	2	8	0	Proposition 3.11 where $n = 6$ , $l = 4$
40	25	8	8	8	3	3	3	2	Proposition 3.6 where $R = GF(25)$
41	25	4	4	16	3	3	9	0	Proposition 3.11 where $n = 5$ , $l = 5$
42	25	4	8	12	3	3	5	0	Proposition 3.7 where $\beta_1=1, \beta_2=2$
43	25	2	2	20	0	0	15	1	Proposition 3.1 $m = 5$ , from $(2,0,1,5)$
44	25	10	10	4	0	0	3	5	Proposition 3.3 where $m = 5$ , from $(2,0,1,5)$
45	26	12	12	1	0	11	0	11	Proposition 3.6 where $R = Z_{26}$

No.	v	$n_1$	$n_2$	$n_3$	$p_{11}^1$	$p_{22}^2$	$p_{33}^3$	$p_{11}^2$	Description
46	26	6	6	13	2	2	0	3	Proposition 3.1 where $m = 2$ , from (6,2,3,13)
47	26	12	12	1	4	4	0	6	Proposition 3.3 where $m = 2$ , from (6,2,3,13)
48	26	4	12	9	0	11	0	1	Proposition 3.8 from (13,4,1)
49	27	6	12	8	1	5	1	2	Proposition 3.10 where $n = 3$
50	27	8	2	16	7	1	7	0	Proposition 3.11 where $n = 9$ , $l = 3$
51	27	4	4	18	1	1	9	2	Proposition 3.1 where $m = 3$ , from (4,1,2,9)
52	27	12	12	2	3	3	1	6	Proposition 3.3 where $m = 3$ , from (4,1,2,9)
53	28	13	1	13	12	0	0	0	Proposition 3.11 where $n = 14$ , $l = 2$
54	28	6	3	18	5	2	10	0	Proposition 3.11 where $n = 7$ , $l = 4$
55	30	14	1	14	13	0	0	0	Proposition 3.11 where $n = 15$ , $l = 2$
56	30	9	2	18	8	1	8	0	Proposition 3.11 where $n = 10$ , $l = 3$
57	30	5	4	20	4	3	12	0	Proposition 3.11 where $n = 6$ , $l = 5$
58	30	3	6	20	0	3	10	1	Proposition 3.1 where $m = 3$ , from (3,0,1,10)
59	30	9	18	2	0	9	1	3	Proposition 3.3 where $m = 3$ , from (3,0,1,10)
60	30	2	2	25	0	0	20	1	Proposition 3.1 where $m = 6$ , from (2,0,1,5)
61	30	12	12	5	0	0	4	6	Proposition 3.3 where $m = 6$ , from (2,0,1,5)

No.	v	$n_1$	$n_2$	$n_3$	$p_{11}^1$	$p_{22}^2$	$p_{33}^3$	$p_{11}^2$	Description
62	30	6	8	15	1	4	0	3	Proposition 3.1 where $m = 2$ , from (6, 1, 3, 15)
63	30	12	16	1	2	8	0	6	Proposition 3.3 where $m = 2$ , from (6, 1, 3, 15)
64	30	14	7	8	13	0	0	0	Proposition 3.8 from (15, 7, 3)
65	31	10	10	10	3	3	3	4	Proposition 3.6 where $R = \mathbf{Z}_{31}$
66	32	15	1	15	14	0	0	0	Proposition 3.11 where $n = 16$ , $\ell = 2$
67	32	7	3	21	6	2	12	0	Proposition 3.11 where $n = 8$ , $\ell = 4$
68	32	5	10	16	0	6	0	2	Proposition 3.1 where $m = 2$ , from (5, 0, 2, 16)
69	32	10	20	1	0	12	0	4	Proposition 3.3 where $m = 2$ , from (5, 0, 2, 16)
70	32	6	9	16	2	4	0	2	Proposition 3.1 where $m = 2$ , from (6, 2, 2, 16)
71	32	12	18	1	4	8	0	4	Proposition 3.3 where $m = 2$ , from (6, 2, 2, 16)
72	32	15	6	10	14	0	0	0	Proposition 3.8 from (16, 6, 2)
73	33	20	10	2	9	9	1	18	Proposition 3.6 where $R = \mathbf{Z}_{33}$
74	34	16	16	1	0	15	0	15	Proposition 3.6 where $R = \mathbf{Z}_{34}$
75	34	8	8	17	3	3	0	4	Proposition 3.1 where $m = 2$ , from (8, 3, 4, 17)
76	34	16	16	1	6	6	0	8	Proposition 3.3 where $m = 2$ , from (8, 3, 4, 17)



No.	v	$n_1$	$n_2$	$n_3$	$p_{11}^1$	$p_{22}^2$	$p_{33}^3$	$p_{11}^2$	Description
77	35	24	6	4	15	5	3	20	Proposition 3.6 where $R = \mathbb{Z}_{35}$
78	35	12	18	4	5	9	0	4	Proposition 3.9 where $n = 7$
79	36	11	2	22	10	1	10	0	Proposition 3.11 where $n = 12, \ell = 3$
80	36	17	1	17	16	0	0	0	Proposition 3.11 where $n = 18, \ell = 2$
81	36	8	3	24	7	2	14	0	Proposition 3.11 where $n = 9, \ell = 4$
82	36	5	5	25	4	4	16	0	Proposition 3.11 where $n = 6, \ell = 6$
83	36	5	10	20	4	4	10	0	Proposition 3.7 where $\beta_1 = 1, \beta_2 = 2$
84	36	10	10	15	4	4	6	2	Proposition 3.7 where $\beta_1 = 2, \beta_2 = 2$
85	36	15	15	5	6	6	0	6	Proposition 3.7 where $\beta_1 = 3, \beta_2 = 3$
86	36	4	4	27	1	1	18	1	Proposition 3.1 where $m = 4$ , from $(4, 1, 2, 9)$
87	36	16	16	3	4	4	2	8	Proposition 3.3 where $m = 4$ , from $(4, 1, 2, 9)$
88	37	12	12	12	2	2	2	5	Proposition 3.6 where $R = \mathbb{Z}_{37}$
89	38	18	18	1	0	17	0	17	Proposition 3.6 where $R = \mathbb{Z}_{38}$
90	38	18	9	10	17	0	0	0	Proposition 3.8 from $(19, 9, 4)$
91	39	24	12	2	11	11	1	22	Proposition 3.6 where $R = \mathbb{Z}_{39}$

No.	v	$n_1$	$n_2$	$n_3$	$p_{11}^1$	$p_{22}^2$	$p_{33}^3$	$p_{11}^2$	Description
92	39	6	6	26	2	2	13	3	Proposition 3.1 where $m = 3$ , from $(6,2,3,13)$
93	39	18	18	2	6	6	1	9	Proposition 3.3 where $m = 3$ , from $(6,2,3,13)$
94	40	19	1	19	18	0	0	0	Proposition 3.11 Where $n = 20$ , $\ell = 2$
95	40	9	3	27	8	2	16	0	Proposition 3.11 where $n = 10$ , $\ell = 4$
96	40	7	4	28	6	3	18	0	Proposition 3.11 where $n = 8$ , $\ell = 5$
97	40	3	6	30	0	3	20	1	Proposition 3.1 where $m = 4$ , from $(3,0,1,10)$
98	40	12	24	3	0	12	2	4	Proposition 3.3 where $m = 4$ , from $(3,0,1,10)$
99	40	2	2	35	0	0	30	1	Proposition 3.1 where $m = 8$ , from $(2,0,1,5)$
100	40	16	16	7	0	0	6	8	Proposition 3.3 where $m = 8$ , from $(2,0,1,5)$
101	42	20	1	20	19	0	0	0	Proposition 3.11 where $n = 21$ , $\ell = 2$
102	42	13	2	26	12	1	12	0	Proposition 3.11 where $n = 14$ , $\ell = 3$
103	42	5	6	30	4	5	20	0	Proposition 3.11 where $n = 6$ , $\ell = 7$
104	42	5	20	16	0	19	0	1	Proposition 3.8 from $(21,5,1)$
105	42	10	10	21	3	5	0	6	Proposition 3.1 where $m = 2$ , from $(10,3,6,21)$
106	42	20	20	1	6	10	0	12	Proposition 3.3 where $m = 2$ , from $(10,3,6,21)$
107	43	14	14	14	3	3	3	6	Proposition 3.6 where $R = Z_{43}$

No.	v	n <sub>1</sub>	n <sub>2</sub>	n <sub>3</sub>	$p_{11}^1$	$p_{22}^2$	$p_{33}^3$	$p_{11}^2$	Description
108	44	21	1	21	20	0	0	0	Proposition 3.11 where $n = 22, \ell = 2$
109	44	10	3	30	9	2	18	0	Proposition 3.11 where $n = 11, \ell = 4$
110	45	4	8	32	3	7	21	0	Proposition 3.11 where $n = 5, \ell = 9$
111	45	14	2	28	13	1	13	0	Proposition 3.11 where $n = 15, \ell = 3$
112	45	4	4	27	1	1	27	1	Proposition 3.1 where $m = 5$ , from $(4, 1, 2, 9)$
113	45	20	20	4	20	20	3	10	Proposition 3.3 where $m = 5$ , from $(4, 1, 2, 9)$
114	45	2	2	40	0	0	35	1	Proposition 3.1 where $m = 9$ , from $(2, 0, 1, 5)$
115	45	18	18	8	0	0	7	9	Proposition 3.3 where $m = 9$ , from $(2, 0, 1, 5)$
116	45	6	8	30	1	4	15	3	Proposition 3.1 where $m = 3$ , from $(6, 1, 3, 15)$
117	45	18	24	2	3	12	1	9	Proposition 3.3 where $m = 3$ , from $(6, 1, 3, 15)$
118	46	22	1	22	21	0	0	0	Proposition 3.11 where $n = 23, \ell = 2$
119	46	22	11	12	21	0	0	0	Proposition 3.8 from $(23, 11, 5)$
120	48	2	15	30	1	14	14	0	Proposition 3.11 where $n = 3, \ell = 16$
121	48	5	7	35	4	6	24	0	Proposition 3.11 where $n = 6, \ell = 8$
122	48	11	3	33	10	2	20	0	Proposition 3.11 where $n = 12, \ell = 4$
123	48	23	1	23	22	0	0	0	Proposition 3.11 where $n = 24, \ell = 2$
124	48	5	10	32	0	6	16	2	Proposition 3.1 where $m = 3$ , from $(5, 0, 2, 16)$

No.	v	$n_1$	$n_2$	$n_3$	$p_{11}^1$	$p_{22}^2$	$p_{33}^3$	$p_{11}^2$	Description
125	48	15	30	2	0	18	1	6	Proposition 3.3 where $m = 3$ , from (5,0,2,16)
126	48	6	9	32	2	4	16	2	Proposition 3.1 where $m = 3$ , from (6,2,2,16)
127	48	18	27	2	6	12	1	6	Proposition 3.3 where $m = 3$ , from (6,2,2,16)
128	49	16	16	16	6	6	6	5	Proposition 3.6 where $R = GF(49)$
129	49	6	6	36	5	5	25	0	Proposition 3.11 where $n = 7$ , $l = 7$
130	49	6	12	30	5	5	17	0	Proposition 3.7 where $\beta_1 = 1$ , $\beta_2 = 2$
131	49	12	12	24	5	5	11	2	Proposition 3.7 where $\beta_1 = 2$ , $\beta_2 = 2$
132	49	12	18	18	5	7	7	2	Proposition 3.7 where $\beta_1 = 2$ , $\beta_2 = 3$
133	49	6	18	24	0	7	11	0	Proposition 3.7 where $\beta_1 = 1$ , $\beta_2 = 3$
134	50	4	9	36	3	8	24	0	Proposition 3.11 where $n = 5$ , $l = 10$
135	50	24	1	24	23	0	0	0	Proposition 3.11 where $n = 25$ , $l = 2$
136	50	8	16	25	3	9	0	2	Proposition 3.1 where $m = 2$ , from (8,3,2,25)
137	50	16	32	1	6	18	0	4	Proposition 3.3 where $m = 2$ , from (8,3,2,25)
138	50	12	12	25	5	5	0	6	Proposition 3.1 where $m = 2$ , from (12,5,6,25)
139	50	24	24	1	10	10	0	12	Proposition 3.3 where $m = 2$ , from (12,5,6,25)
140	50	24	9	16	23	0	0	0	Proposition 3.8 from (2,5,9,3)



# REFERENCES

1. A. A. Albert and R. Sandler, An Introduction to Finite Projective Planes, Holt, Rinehart and Winston, 1968.
2. F. R. Albrecht, Strongly Regular Graphs with Few Vertices, Thesis, The Ohio State University, 1971.
3. W. C. Blackwelder, On constructing balanced incomplete block designs from association matrices with special reference to association schemes of two and three class, J. Combinatorial Theory, 7 (1969), 15-36.
4. R. C. Bose, Strongly regular graphs, partial geometries, and partially balanced designs, Pacific J. Math, 13 (1963), 389-419.
5. R. C. Bose and D. M. Mesner, On linear associative algebras corresponding to association schemes of partially balanced designs, Ann. Math. Stat., 30 (1959), 21 - 38.
6. R. C. Bose and K. R. Nair, Partially balanced incomplete block designs, Sankhyā, 4 (1939), 337-372.
7. R. C. Bose and T. Shimamoto, Classification and analysis of partially balanced incomplete block designs with two associate classes, J. Amer. Stat. Assn. 47 (1952), 151-184.
8. P. Dembowski, Finite Geometries, Springer-Verlag, New York, 1968.
9. M. Hall, Jr., Combinatorial Theory, Blaisdell, Waltham, Mass., 1967.
10. R. Laskar, Finite nets of dimension three, Proceedings of the Second Chapel Hill Conference on Combinatorial Mathematics and its Applications, Univ. of N. Carolina at Chapel Hill, 1970.